McAfee Total Protection Service Product Guide

COPYRIGHT

Copyright © 2010 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

License Attributions

Refer to the product Release Notes.

Contents

Introducing Total Protection Service 8

How Total Protection Service works 9

Types of protection 9

Core product strengths 10

New features for this release 11

The role of the client software 11

Updates to the client software 12

Overview of update methods 13

Simple updates through direct connections 14

Updates using Rumor technology 14

Updates through relay servers 14

Management with the SecurityCenter 15

Create user groups 16

Customize policies 17

Check reports 19

Using the Client Software 20

How to access the client software. 20

About the icon 21

About the console 22

Types of client software updates 22

Terminal server support 24

Specifying when computers check for updates 24

Updating client computers manually 24

Disabling updates for non-logged on users 25

Performing setup and maintenance tasks 25

Testing virus protection 25

Changing the language for the software 26

Logging on as a site administrator 26

Configuring notifications 26

Configuring what users see 27

Uninstalling the client software 27

Frequently asked questions 28

Error messages 28

Using the SecurityCenter 30

The SecurityCenter 30

Logging on to the SecurityCenter 31

Accessing data on SecurityCenter pages 32

Protection status at a glance....33
Viewing protection at a glance....34
Working with widgets....35
Management of client computers....36
Working with computers....37
Working with an individual computer....38
Management of computer groups....39
Working with groups....40
Management of Active Directory groups....41
Downloading the Active Directory Synchronization utility....41
Importing Active Directory groups....41
Installing on Active Directory groups....42
Synchronizing Active Directory groups....43
Viewing the synchronization status....43
Viewing the Active Directory tree in the SecurityCenter....43
Management of group administrators....44
Working with group administrators....45
Management of security policies....46
McAfee Default policy....47
Working with policies....51
Generation of security reports....51
Scheduling reports....53
Adding your logo to reports....54
Computer Profiles report....54
Duplicate Computers report....55
Managing your account....56
Configuring your account profile....56
Signing up for email notifications....57
Viewing and updating subscription information....57
Buying and renewing subscriptions and licenses....58
Locating or creating keys for your account....58
Merging accounts....59
Downloading tools and utilities....59
Getting assistance....60
Frequently asked questions about the SecurityCenter....61
Questions about reporting....61
Questions about adding, renewing, and moving licenses....62
Using Virus and Spyware Protection....63
How detections are handled....64

Spyware protection mode and detections....64
Use learn mode to discover programs....65
Types of scans....65
On-access (automatic) scans....65
On-demand scans....66
Email scans....67
Spyware scans....67
Scanning on client computers....68
Scanning on demand from the console....68
Scanning on demand from Windows Explorer....68
Scanning email on client computers....69
Viewing the progress of scheduled scans....69
Enabling and disabling on-access scanning....69
Configuring scanning policy options....70
Scheduling a scan....70
Enabling optional types of virus scans....70
Excluding files and folders from virus scans....71
Selecting spyware scanning options....72
Approving and unapproving programs in a policy....72
Managing detections....73
Viewing scan results on client computers....73
Managing potentially unwanted programs on client computers....74
Viewing quarantined files on client computers....74
Viewing user-approved programs and applications....75
Viewing threats detected on the account....76
Viewing unrecognized programs detected on the account....77
Reports for virus and spyware protection....77
Detections report....78
Unrecognized Programs report....79
Detection History report....79
Best practices (virus and spyware protection)....80
Frequently asked questions....80
Error messages....81
Using Firewall Protection....82
Connection type and detections of incoming communications....83
Custom connections....83
Firewall protection mode and detections of unknown applications....85
Use learn mode to discover Internet applications....86
The role of IP addresses....86

The role of system service ports 86
Standard assignments for system service ports 87
Firewall configuration 87
Interaction between user and administrator policy settings. 89
Configuring policy options 89
Selecting general firewall settings 89
Configuring options for Internet applications 90
Tracking blocked communications 91
Configuring custom connections 91
Configuring system services and port assignments 91
Configuring IP addresses 92
Installing and enabling firewall protection at the policy level 93
Installing firewall protection during policy updates 94
Enabling and disabling firewall protection 94
Managing detections 95
Viewing unrecognized programs detected on the account 95
Viewing user-approved programs and applications 95
Viewing blocked communications 96
Reports for firewall protection 97
Unrecognized Programs report 97
Inbound Events Blocked by Firewall report 97
Best practices (firewall protection) 98
Frequently asked questions 99
Questions about policies 99
Questions about general firewall protection 100
Using Browser Protection and Web Filtering 101
Browser protection features 101
How safety ratings are compiled 102
Safety icons and balloons protect during searches 103
Using site safety balloons 103
Testing communication problems 103
SiteAdvisor menu protects while browsing 104
Using the SiteAdvisor menu 105
Safety reports provide details 105
Viewing safety reports 107
Information that browser protection sends to McAfee 107
Installing browser protection during policy updates 108
Web filtering features 108
Enabling and disabling browser protection via policy 108

Enabling and disabling protection at the client computer 109
Block and warn sites by safety ratings 109
Blocking or warning site access based on safety ratings..... 111
Blocking or warning file downloads based on safety ratings 111
Blocking phishing pages 112
Block and warn sites by content..... 112
Blocking or warning site access based on content 113
Authorize and prohibit sites by URL or domain..... 113
How site patterns work..... 114
Adding authorized and prohibited sites 115
Customizing messages for users 115
Viewing browsing acitivity..... 116
Web Filtering report 117
Best practices (browser protection) 117
Frequently asked questions..... 118

Introducing Total Protection Service

Total Protection Service provides a "hands-off" solution to safeguard the computers on your network automatically by keeping itself up-to-date and checking for threats contained in files and programs, in email messages, in communications from inside and outside the network, and on websites.

When you purchase a subscription to Total Protection Service, an account is created for you, and you become the account administrator (referred to as the *site administrator*). When you install the Total Protection Service client software on computers, they are added to your account. A weekly email alerts you to any problems detected for computers on your account.

NOTE: In some organizations, another person, such as a purchasing department representative, purchases the subscription and then designates you to be the site administrator.

For a more "hands-on" approach, use the SecurityCenter to view and manage computers and detections on your network. Your service provider sends you a unique URL and login credentials for your account, which you can use to access the SecurityCenter. This is a pre-configured website that provides a simple-to-use management console for monitoring the protection status of computers on your account. Use the SecurityCenter to view reports on detections and activities and to configure security settings that address the specific needs of your account.

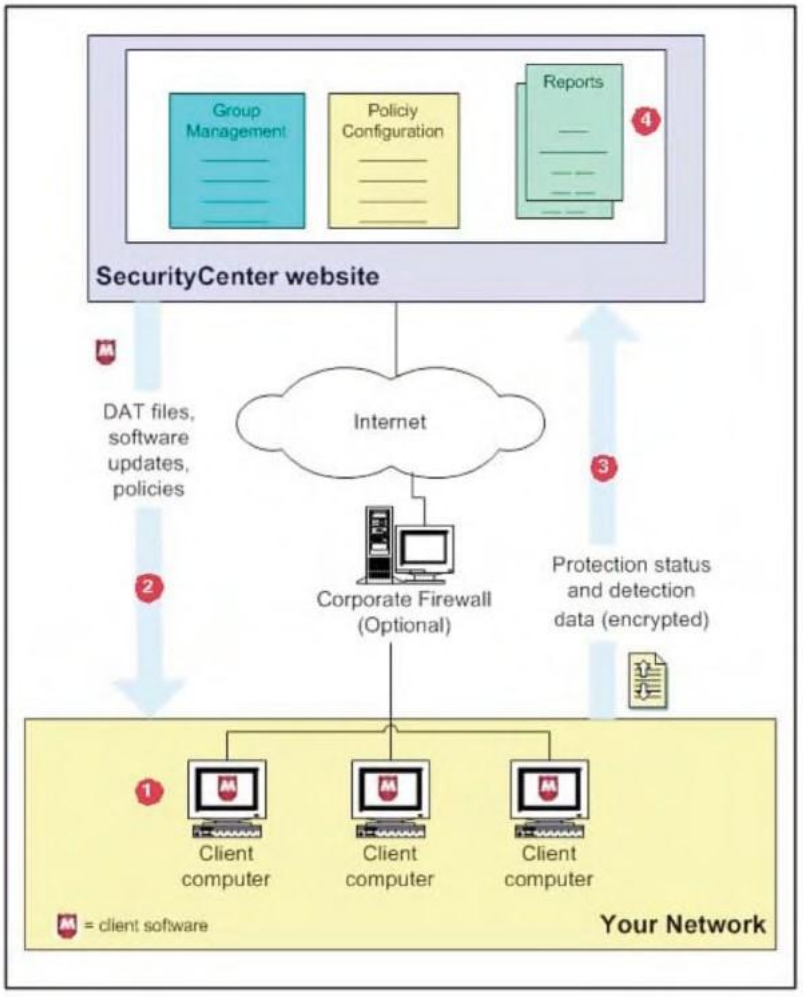
This section provides an overview of the product and its features.

Contents

- How Total Protection Service works
- Types of protection
- Core product strengths
- New features for this release
- The role of the client software
- Updates to the client software
- Management with the SecurityCenter

How Total Protection Service works

Total Protection Service delivers comprehensive security as a service for all the computers on your account. It automatically checks for threats, intercepts them, takes the appropriate action to keep your data and your network safe, and tracks detections and security status for reports.



1	Client software runs on each computer where it is installed.
2	The client software up dates itself — automatically and silently — by downloading the latest detection definition (DAT) files from your account's administrative website, the McAfee Security Center. DAT files define the threats that the client software detects.
3	The client software uploads security information about each computer to the Security Center for use in administrative reports.
4	As your account's administrator, you can use a web browser to visit the Security Center, where you can access reports that detail the status of client computers and use tools for customizing and managing security.

Types of protection

The core features in Total Protection Service safeguard against a broad range of threats.

Feature	Description
Virus and spyware protection	Checks for viruses, spyware, unwanted programs, and other potential threats borne on removable media or brought in from your network, including via email. Every time a file on your computer is accessed, virus and spyware protection scans the file to make sure it is free of viruses and spyware.
Firewall protection	Establishes a barrier between each computer and the Internet or other computers on your local network. It silently monitors communications traffic for suspicious activity and takes appropriate action, such as blocking.
Browser protection	Displays information to safeguard client computer users against web-based threats. Users can view website safety ratings and safety reports as they browse or search with Microsoft Internet Explorer or Mozilla Firefox.
McAfee SecurityCenter	Provides centralized access to status information and management tasks for your account.

Core product strengths

Total Protection Service safeguards your computers with:

- **Continuous protection** — From the time a client computer is turned on until it is turned off, Total Protection Service silently monitors all file input and output, downloads, program executions, inbound and outbound communications, and other system-related activities.

- **Instant discovery for virus threats** — When Total Protection Service detects a virus threat, it attempts to clean the item containing the threat before further damage can occur. If an item cannot be cleaned, a copy of it is placed in a quarantine folder and the original item is deleted.

- **Customized threat response for program detections** — By default, Total Protection Service provides a high degree of protection against threats. You can also configure the response to detections of potentially unwanted programs and suspicious activity to suit your needs: take immediate action to clean, quarantine, or block the detection; prompt users for a response; or only log the detection for administrative reports.

- **Preemptive safety notificationsfor web-based threats** — Threats reported on websites are communicated to users through color-coded icons and safety reports, enabling them to minimize exposure to dangerous websites.

- **Automatic updates** — Total Protection Service checks for product updates at regular intervals throughout the day, comparing security components against the latest releases. When a computer needs a newer version, the client software retrieves it automatically.

- **Avert Early Warning system and outbreak response** — Total Protection Service uses the latest information about threats and outbreaks as soon as they are discovered by McAfee Avert® Labs, a research division of McAfee. Whenever Avert Labs releases an outbreak detection definition (DAT) file, computers on your account receives it promptly.

New features for this release

Core features

All versions of Total Protection Service include these new features to facilitate account management.

Now you can do this...	Details
Customize the SecurityCenter home page	Select the summary and activity reports (known as *widgets*) that appear on the Dashboard page. Click and drag to reposition and resize widgets.
Get real-time evaluation for unrecognized threat detections	Artemis technology sends unrecognized detections to McAfee Avert Labs for evaluation.
Schedule reports	Customize the data that appears in reports, then automatically generate and email these reports at regular intervals.
Designate a default policy for your account	Select a customized policy as the default assigned to computers in your account.
Display computers by policy	Organize the computer listing for your account by policy as well as by groups.
Access more account data on the SecurityCenter	Look up your company key, grant number, installation URL, and group IDs more easily.

Additional types of protection

Some versions of Total Protection Service offer additional types of protection that extend coverage to other network assets.

Now you can do this...	Details
Control access to websites based on their safety ratings and content	Web filtering works within browser protection to add policy and reporting options. You can block user access to websites and file downloads or warn them about reported threats, customize messaging that displays for blocked sites, create lists of authorized and prohibited websites based on their domain or URL, or view a report of web browsing activity on your network.
Scan websites for vulnerabilities	Vulnerability scanning enables you to register IP addresses, then scan them for vulnerabilities and report scan results to the SecurityCenter in alerts.
Access protection portals without separate login credentials	The single sign-on feature lets you open the email protection or vulnerability scanning portal directly from the SecurityCenter, without entering additional login credentials.

The role of the client software

The Total Protection Service software installed on client computers implements a three-prong approach to security by:

1 Silently monitoring all file input and output, downloads, program executions, inbound and outbound communications, and other system-related activities on client computers. As a result of this monitoring, the client software automatically:

- Deletes or quarantines detected viruses.
- Removes potentially unwanted programs, such as spyware or adware, unless you select a different response.
- Blocks suspicious activity unless you specify a different response.
- Indicates unsafe websites with a color-coded button or icon in the browser window or search results page. These indicators provide access to safety reports that detail site-specific threats.

2 Regularly updating detection definition (DAT) files and software components to ensure that you are always protected against the latest threats.

3 Uploading security information for each client computer to the SecurityCenter, then using this information to send emails and create reports that keep you informed about your account's status.

Updates to the client software

Regular updates are the cornerstone of Total Protection Service. The client software periodically checks a site on the Internet for newer versions of these software components.

- Regular DAT files, which contain the latest definitions for viruses, potentially unwanted programs, and cookies and registry keys that might indicate spyware. These are updated regularly to add protection against new threats.
- Outbreak DAT files, which are high-priority detection definition files released in an emergency situation in response to a specific new threat.
- Upgrades to the software.
- Policy updates.
- Updates of its software components running on client computers.
- Updates to the security data maintained on the SecurityCenter website and used in administrative reports.

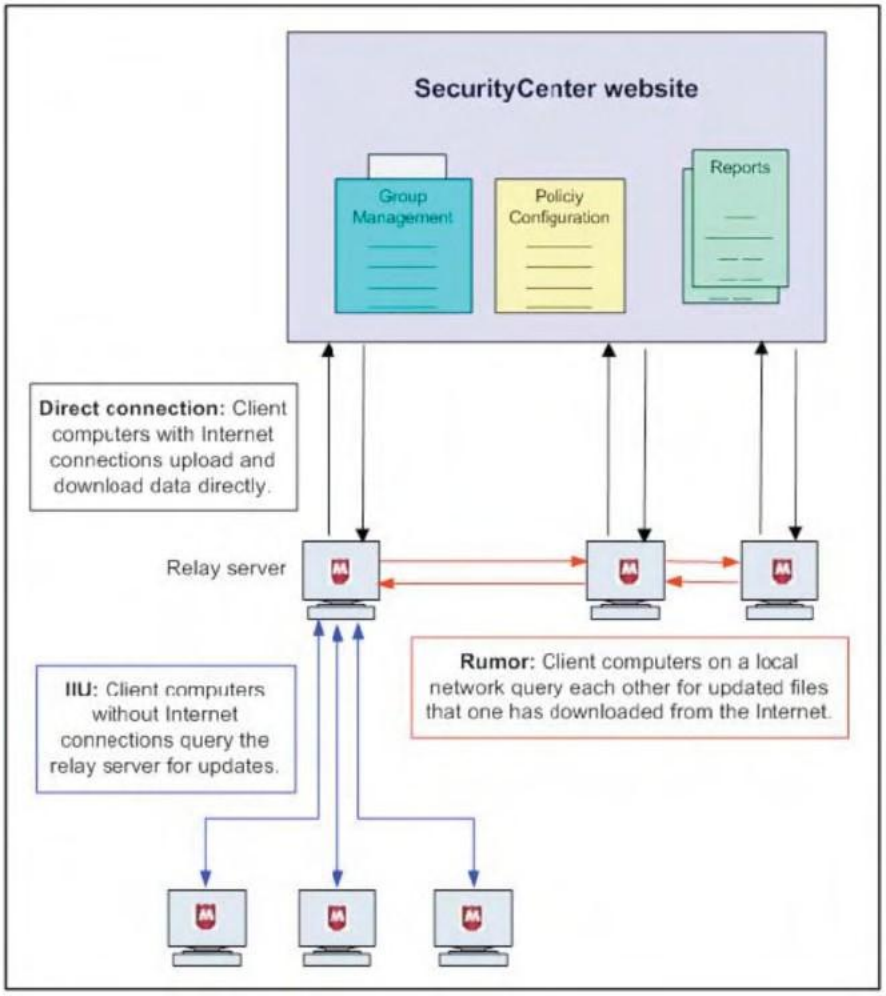
At the same time, the client software sends information about its detections and protection status, to update the security data maintained on the SecurityCenter website and used in administrative reports.

Overview of update methods

Five minutes after a client computer connects to the network, and at regular intervals throughout the day, the Total Protection Service client software checks for updates. If updates are available, the client computer retrieves them.

In addition, users can check for updates manually at any time by clicking the Total Protection Service icon in the system tray, then selecting **Update Now**.

Updates can occur in three ways. You can implement one method or a combination of methods, which enables you to tune the impact updates have on network resources.



1. For simple updates, each client computer on your account has a direct connection to the Internet and checks for new updates.
2. Rumor technology enables all computers in a workgroup to share downloaded files, which controls Internet traffic and minimizes expensive downloads.
3. Internet Independent Updating (IIU) enables any computer on the network to get information from the update site, even if that computer does not have an Internet connection, by communicating with the update site through a network computer that is configured as a relay server.

Simple updates through direct connections

Each client computer that has a direct Internet connection can check for updates and download them from the update site on the Internet. This is the simplest method of retrieving updates.

Updates using Rumor technology

When one computer shares updates with other computers on the local area network (LAN), rather than requiring each computer to retrieve updates from the update website individually, the Internet traffic load on the network is reduced. This process of sharing updates is called Rumor.

1. Each client computer checks the version of the most recent catalog file on the Internet site. This catalog file contains information for every component in the Total Protection Service client software, and is stored in a digitally signed, compressed .cab file format.
   - If the version is the same as the catalog file on the client computer, the process stops here.
   - If the version is different from the catalog file on the client computer, the client computer attempts to retrieve the latest catalog file from its peers. It queries if other computers on the LAN have already downloaded the new catalog file.
2. The client computer retrieves the required catalog file (directly from the Internet site or from one of its peers) and uses it to determine if new components are available for Total Protection Service.
3. If new components are available, the client computer attempts to retrieve them from its peers. It queries whether computers on the LAN have already downloaded the new components.
   - If so, the client computer retrieves the update from a peer. (Digital signatures are checked to verify that the computer is valid.)
   - If not, the client computer retrieves the update directly from the update site.
4. On the client computer, the catalog file is extracted and new components are installed.

Updates through relay servers

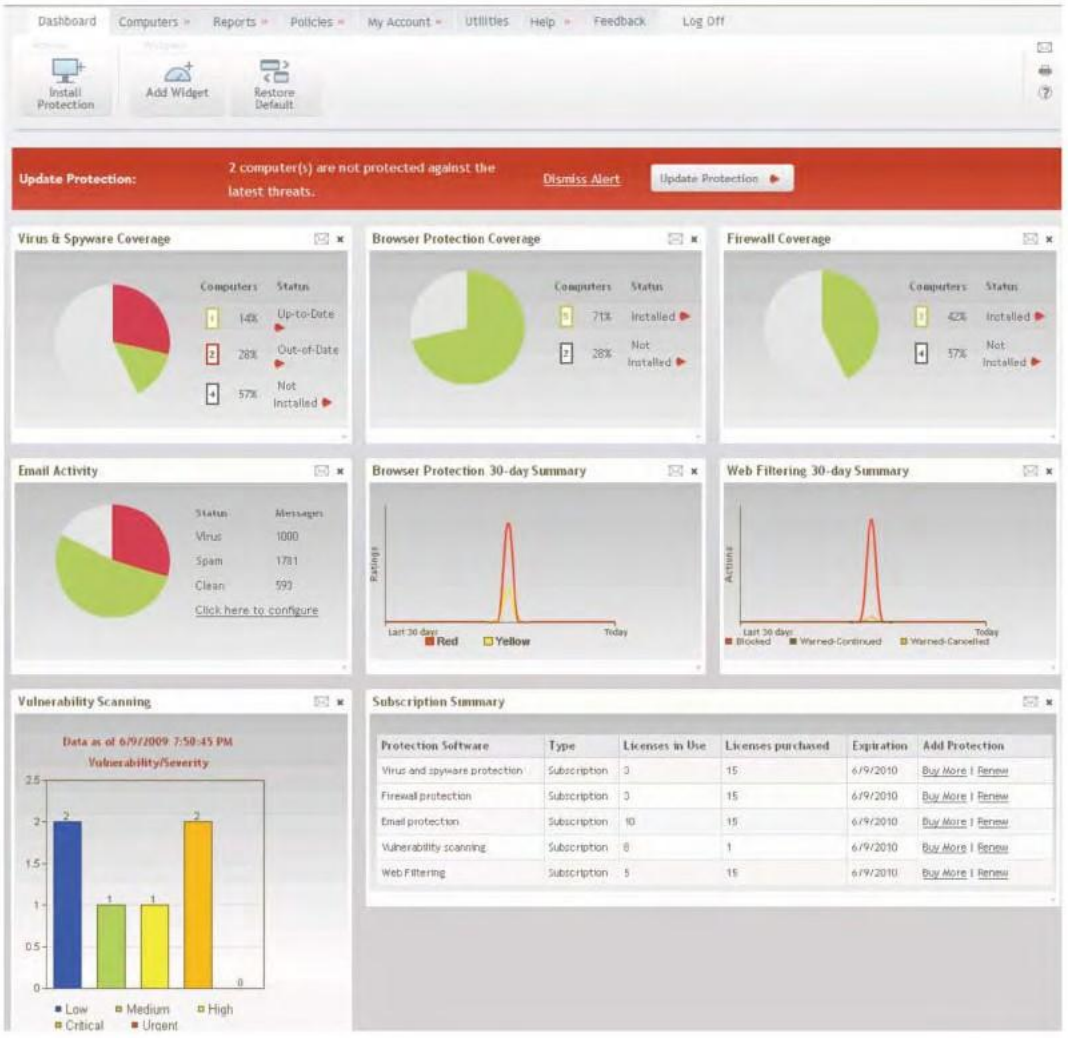
Internet Independent Updating (IIU) enables computers to update Total Protection Service client software when they are not connected to the Internet. At least one computer on the subnet must have an Internet connection to be able to communicate with the update site. That computer is configured to act as a relay server, and computers without an Internet connection use this computer to connect with the Internet and retrieve updates directly from the McAfee update site.

1. When a computer without Internet access fails to connect directly to the update site, requests a response from a relay server on the LAN and uses that computer to communicate with the update site.
2. The computer without an Internet connection downloads updates directly from the update site through the relay server.

You can specify which computers function as relay servers when you install the client software or at a later time. See the installation guide for more information.

Management with the SecurityCenter

Your service provider sends you a unique URL and login credentials for your account, which you can use to log on to the SecurityCenter. From the SecurityCenter, you can access management tools to monitor the status of computers on your account and configure security settings that address the specific needs of your account.



The Dashboard page is the "home page" of the SecurityCenter. It shows summary information for your account at-a-glance.

- **Alerts and action items** — Indicate whether any action is required to address security issues, and links you to instructions for resolving them.
- **Product coverage and activity summaries** — Modular reports (known as *widgets*) illustrate the current status of your account. These include reports on protection coverage (such as computers where protection is installed and enabled) and activity (such as the number of detections, emails, and website visits). The type, size, and placement of widgets can be customized.

- **Subscription tracking** — Widgets are available to show subscription and licensing information for your account. Click a button to install protection, create a trial subscription, renew or purchase a subscription, or buy additional licenses.
- **Links to related portals** — Some widgets contain a link to a portal used for managing non-client-based protection, such as email protection and vulnerability scanning.

The SecurityCenter offers two powerful tools for protecting and monitoring displaying your computers and fine-tuning their security settings.

- **User groups**: Create groups for computers that have one or more common characteristics. This enables you to view and manage them as a single entity when needed.
- **Customized policies**: Select settings for protection features, save them in a policy, and assign the policy to computers or groups of computers. This enables you to configure settings targeted specifically for each computer's environment and risk factors.

From the SecurityCenter, access important information and additional management tools.

- Installation wizard and links to remote installation methods.
- Detailed identification, activity, and detection data for the groups and computers on your account.
- Administrative reports.
- Policy configuration tools.
- Account configuration, reference information, and subscription status.
- Helpful utilities.
- Product documentation and links to product support and demos.

Create user groups

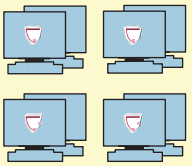
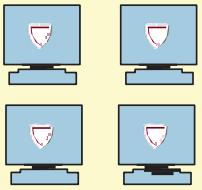
A group consists of one or more computers that share a particular feature. Each computer running the client software belongs to a group. By default, computers are placed in the Default Group.

In large accounts, groups are an essential tool for managing computers because they let you manage different types of computers more easily. You can view all the computers in a group, view detections and reports for the group, and assign security settings (called *policies*) to a group as a single entity rather than individually. You can base groups on geographic location, department, computer type, user tasks, or anything meaningful to your organization.

For example, you might place all laptops used by traveling sales representatives into a single group called Sales Team. You can then view details about this group of computers separately from other computers in your account. You can easily check detections for these computers or customize their security settings to protect them from the risks specific to users of public networks.

To create groups, use the **Computers** tab on the SecurityCenter website.

The following example shows how an administrator might configure policies for client computers in three different groups. You should configure policies for your users to meet your own company's needs.

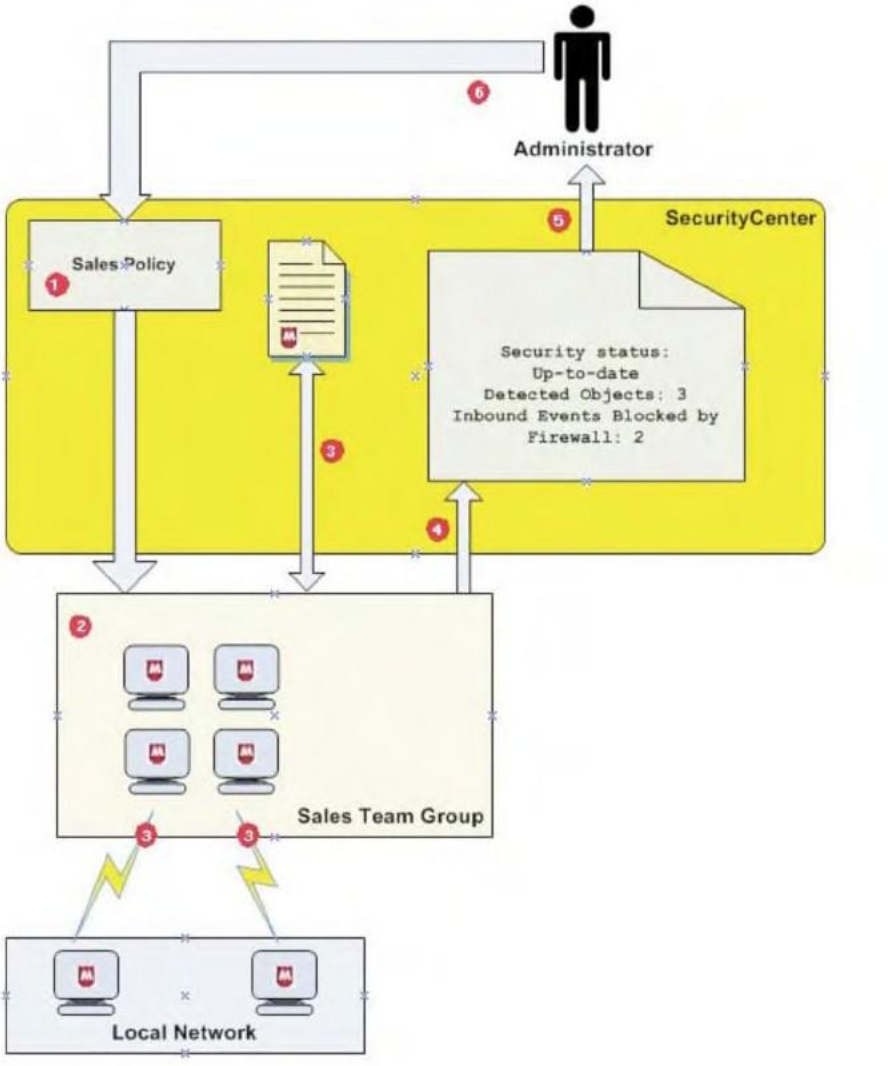
Policy setting	Home Office Group On-site client computers 	Sales Team Group Laptops 	Administrative Group Site and group administrators 
On-Demand Scan	Weekly	Daily	Daily
Enable outbreak response	Enabled	Enabled	Enabled
Scan within archives during on-access scans	No	Enabled	Enabled
Check for updates every	12 hours	4 hours	4 hours
Spyware Protection Mode	Prompt	Protect	Prompt
Approved Programs	None	None	Nmap remote admin tool
Firewall Protection Mode	Protect	Protect	Prompt
Use Smart Recommendations to automatically approve common Internet applications	Enabled	No	Enabled
Connection Type	Trusted network	Untrusted network	Trusted network
Allowed Internet Applications	AOL Instant Messenger	None	• AOL Instant Messenger • GoogleTalk
Access to Sites, Access to Downloads (Web Filtering)	• Red — Block • Yellow — Warn • Unrated — Warn	• Red — Block • Yellow — Block • Unrated — Warn	• Red — Warn • Yellow — Allow • Unrated — Allow
Block phishing pages (Web Filtering)	Enabled	Enabled	Enabled

Customize policies

After installation, Total Protection Service protects client computers from threats immediately by using the security settings configured in the McAfee Default policy. However, you might want to change the way some features are implemented for some or all of the computers on your account. For example, you might want to set up a list of programs you consider safe or have computers check for updates every four hours.

Policies are made up of security settings that define how the client software operates on client computers. Policy management allows you to assign different levels and types of protection to different users. If you have created groups, you can assign a unique policy to each group or one policy to all groups.

For example, you can assign a Sales policy to your mobile Sales Team group, with security settings that protect against threats in unsecured networks such as airports and hotels.



1	Create a Sales Team group and a Sales policy.
2	Assign the Sales policy to the computers in the Sales Team group.
3	Client software running on computers in the Sales Team group performs the tasks defined in the Sales policy: • Check for updates to software components and DAT files every 4 hours. • Check for an outbreak DAT file every hour. • Scan for viruses and potentially unwanted programs daily. • Block communication from computers on the local network (untrusted network).
4	Client software sends security data for each client computer to the SecurityCenter.
5	Administrator checks the security status for the Sales Team group in reports on the SecurityCenter.
6	The administrator adjusts the Sales policy. The modified policy is downloaded automatically to client computers in the Sales Team group the next time they check for updates.

Check reports

Whenever client computers check for updates, they upload information about their security status to the SecurityCenter. This information includes the number and type of detections, the functional status of the client software, and any applications or communications that were approved by users or blocked. The method used to upload information is the same method used to retrieve updates (i.e., through a direct connection, Rumor technology, or a relay server).

A summary of this information is sent to you in a weekly status email (unless you or your service provider has disabled this feature). You can also retrieve detailed information in reports available on the SecurityCenter. Reports show the types of detections and activities occurring for computers on your account. Use them to evaluate the current policy options for your account and adjust them as needed.

You can also schedule these reports to run at regular intervals and be delivered to you or other specified persons as an email attachment.

Using the Client Software

Total Protection Service client software is installed on each computer you want to protect. When installation is complete, the computer is added to your Total Protection Service account automatically. The software then runs in the background to download updates to the computer, protect the computer from threats, and send detection data to the SecurityCenter for use in administrative reports.

Typically, users have little interaction with the client software unless they want to manually scan for threats. User tasks are documented in the online user help on client computers.

As an administrator, you can use the SecurityCenter website to configure settings and monitor detections for the client computers on your account. Occasionally, you might work directly on a client computer by using the tasks described in this section.

Contents

- ▶ How to access the client software
- ▶ Types of client software updates
- ▶ Performing setup and maintenance tasks
- ▶ Frequently asked questions
- ▶ Error messages

How to access the client software

Total Protection Service has two visual components through which users interact with the client software:

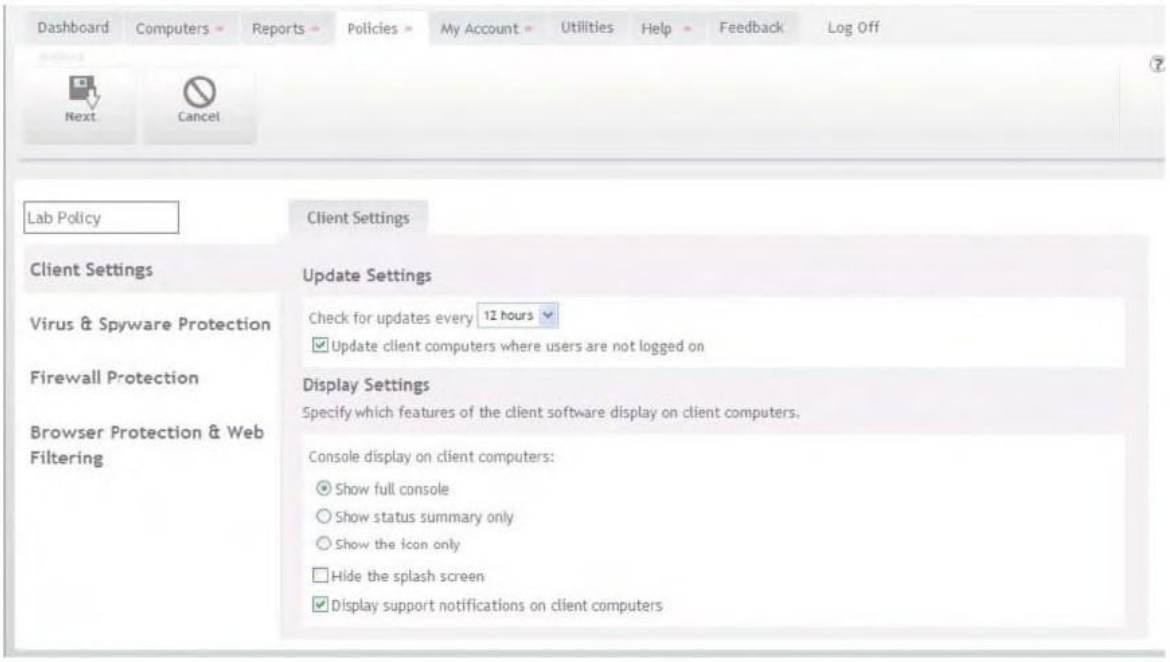
An icon that appears in the Windows system tray.

- A console that displays the current protection status and provides access to features.

You, the administrator, determine which components appear by configuring policy options on the SecurityCenter website and assigning them to client computers. The options are:

- Icon only, which enables users to access only a limited set of features. They can view the status of the software (for example, when downloads are occurring) and perform manual updates.
- Icon and protection status summary, which allows access to a limited set of features.
- Icon and full console, which allows access to all features. This is the default setting.

Access these policy options on the **Policies** page under **Client Settings**.



About the icon

The Total Protection Service icon appears in the Windows system tray. It provides access to the product's console and to some of the basic tasks you might need to perform.

Use the icon to:

- Check for product updates.
- Open the console, to check the protection status and access features. (Available if the administrator has configured this option.)
- Activate your copy of the software.
- Renew the subscription or buy more licenses.

How the icon indicates the status of the client software

The appearance of the icon changes to indicate the status of the client software. Hold your cursor over the icon to display a message describing the current condition.

This icon...	...indicates:
	Total Protection Service is active and there are no issues to be aware of.
	An update is in progress. Do not interrupt your Internet or LAN connection; do not log off your computer.
	One of these conditions exists: • Your Total Protection Service subscription is expired. Renew it or contact your administrator. • Your pre-installed or trial subscription is not activated. • Firewall protection is disabled.

This icon...	...indicates:
	• The last update failed to complete. Check your Internet or LAN connection and perform a manual update (click the icon, then select **Update Now**). • On-access scanning is disabled.

About the console

Check the protection status and access the features of the client software through the console. To display the console, use one of these methods:

- Double-click the Total Protection Service icon in the system tray.
- Click the icon, then select **Open Console**.

Click **Start | Programs | McAfee | Managed Services | Total Protection Service**.

The basic console displays the status of the protection features installed on the computer.

- Detected risks are highlighted in red. Click **Fix** to resolve the risk.
- To access product features and perform tasks, click **Action Menu**, then select from the options:
  - **Product Details** — Display the full console with links to features and tasks.
  - **Scan Computer** — Select a scan target and begin scanning for threats.
  - **Set Connection Type** — Specify the type of network the computer connects to. This determines which communications firewall protection allows to access the computer.
  - **View Application List** — Specify applications that are allowed to access the Internet or blocked.
  - **Admin Login** — Log on as an administrator to access administrative features. Requires site administrator credentials.
  - **View Help** — Display online help.

NOTE: The client features you can access are determined by policy options assigned to the computer.

Types of client software updates

Regular updates are the cornerstone of Total Protection Service. To perform updates, the client software connects directly to a site on the Internet and checks for:

- Updates to the detection definition (DAT) files used to detect threats. DAT files contain definitions for threats such as viruses and spyware, and these definitions are updated as new threats are discovered.
- Upgrades to software components. (To simplify product terminology, both updates and upgrades are referred to as updates.)

Updates usually occur automatically in the background. Even computers without Internet access can retrieve updates through relay servers. In addition, users can perform on-demand (manual) updates at any time, and you can configure optional policy settings for updating tasks.

Client software is updated in these ways.

Type of update	Description
Automatic updates	The software on each client computer automatically connects to the Internet directly or through a relay server and checks for updated components. Total Protection Service checks for updates five minutes after a user logs on and at regular intervals thereafter. For example: • If a computer is normally connected to the network all the time, it checks for updates at regular intervals throughout the day. • If a computer normally connects to the network each morning, it checks for new updates five minutes after the user logs on each day, then at regular intervals throughout the day. • If a computer uses a dial-up connection, the computer checks for new updates five minutes after dialing in, then at regular intervals throughout the day. By default, computers check for new updates every 12 hours. You can change this interval by configuring a policy setting. NOTE: Automatic updates do not work: • On computers where a CHAP or NTML proxy is set up in Internet Explorer. • When no user is logged on to a computer without an Internet connection that receives updates using a relay server. Pre-installed and CD-based versions of Total Protection Service need to be activated before automatic updates occur. See the online user help for more information.
Manual updates	At times, users might want to check for updates manually. For example, when a computer appears to be out-of-date in your administrative reports, users might need to update manually as part of the troubleshooting process.
Outbreak updates	When an outbreak is identified by McAfee Avert Labs, they issue an outbreak DAT, which is a special detection definition (DAT) file marked as **Medium** or **High** importance. It is specially encoded to inform the first computer receiving it to share the update immediately with other client computers on the network. NOTE: In rare cases, McAfee might send an EXTRA.DAT file with instructions for manually installing it. For maximum protection, configure your policies to check for an outbreak DAT file every hour. This feature is enabled by default.
Updates when no user is logged on	In most scenarios, Total Protection Service supports terminal servers and the Windows fast user switching feature. When an update occurs, one session is designated as the primary update session. A pseudo user is defined, which enables automatic updates to occur on computers where no user is logged on. For certain configurations, automatic updates cannot occur. Total Protection Service cannot create the pseudo user when: • The computer is a domain controller. • Local security policies, including password restrictions, prevent the user's creation. • The computer receives updates through a relay server and no one is logged on. When the pseudo user cannot be created, automatic updates do not occur. The pseudo user also cannot update if the computer is behind an authenticating proxy server or on computers where a CHAP or NTML proxy is set up in Internet Explorer.

Terminal server support

Total Protection Service supports updates for terminal servers and the Windows fast user switching feature in most scenarios, with these limitations:

- When an update occurs on a terminal server, one session is designated as the primary update session for restrictions that apply to automatic updates.
- For all user sessions, the Total Protection Service icon is removed from the system tray during the installation or update. The icon is restarted only for the user logged on to the primary update session. All user sessions are protected, and other users can manually redisplay their icons by clicking **Start | Programs | McAfee | Managed Services | Total Protection Service**.
- Detection notifications are not displayed on the desktop of all computer users if the fast user switching feature is enabled.

Specifying when computers check for updates

For virus and spyware scans to detect all the latest threats, the detection definition (DAT) files must be kept up-to-date. DAT files are updated by McAfee Avert Labs whenever new threats are discovered.

Use this task to select how often client computers check for updates to software components and DAT files. By default, they check every 12 hours.

Task

For option definitions, click **?** in the interface.

1. In the SecurityCenter, click the **Policies** tab, then click **Add Policy** (or click **Edit** to modify an existing policy).
2. Click **Client Settings**.
3. On the Client Settings tab, under Update Settings, select a frequency from the **Check for updates every** list.
4. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Updating client computers manually

Use this task to check for and download updates to detection definition (DAT) files and software components. Manual updates are also called on-demand updates.

Task

- Click the Total Protection Service icon in the system tray, then select Update Now.
  - A panel shows the progress of the update.
  - When the update is completed, the panel displays the date of the last update and a list of files that were downloaded.
  - The panel closes automatically after the update is completed.

Disabling updates for non-logged on users

Use this task to prevent failed automatic updates from being reported as errors when requirements cannot be met for updating computers where no user is logged on.

Task

For option definitions, click **?** in the interface.

1. In the SecurityCenter, click the **Policies** tab, then click **Add Policy** (or click **Edit** to modify an existing policy).
2. Click **Client Settings**.
3. On the Client Settings tab, under Update Settings, deselect **Update client computers where users are not logged on**.
4. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Performing setup and maintenance tasks

Use these tasks to set up and monitor the general features of the Total Protection Service client software.

Tasks

- Testing virus protection
- Changing the language for the software
- Logging on as a site administrator
- Configuring notifications
- Configuring what users see
- Uninstalling the client software

Testing virus protection

Use this task to test the virus-detection feature of virus and spyware protection by downloading the EICAR Standard AntiVirus Test File at the client computer. Although it is designed to be detected as a virus, the EICAR test file is not a virus.

Task

1. Download the EICAR file from the following location:
   http://www.eicar.org/download/eicar.com

   If installed properly, virus and spyware protection interrupts the download and displays a threat detection notification.
2. Click **OK**, then select **Cancel**.

   NOTE: If installed incorrectly, virus and spyware protection does not detect the virus or interrupt the download process. In this case, use Windows Explorer to delete the EICAR test file from the client computer, then reinstall Total Protection Service and test the new installation.

Changing the language for the software

By default, the client software uses the address that was submitted when the client software was purchased or activated to determine the language. (If that language is not supported on the computer, the one most closely matching is used.) Use this task at the client computer to change the language at any time.

Task

1. Click the Total Protection Service icon in the system tray, then select **Open Console**.
2. From the Action Menu, select **Product Details**.
3. In the SecurityCenter Communication area, click **Select Console Language**, select a language, then click **OK**.
4. Select **Use the specified custom language**, then select a language from the drop-down list.
5. Close the console, then re-open it (by repeating step 1). The console appears in the selected language.

Logging on as a site administrator

Use this task to log in to a client computer as a site administrator, which makes the full console and these additional tasks available:

- Viewing the progress of scheduled scans that are in progress.
- Managing files in the Quarantine Viewer.
- Disabling and enabling on-access scanning.
- Logging on to the SecurityCenter.

Task

1. Click the Total Protection Service icon in the system tray, then select **Admin Login**.
2. Type your login credentials for the SecurityCenter. These were sent to you in a Welcome email when you purchased Total Protection Service.
   - **Email address** — The email address used to sign up for Total Protection Service.
   - **Password** — In most cases, the password you created when signing up.
3. Click **Submit**.

Configuring notifications

Use this task to specify whether notifications display on client computers to let users know that support is ending for their operating system. By default, Total Protection Service displays notifications:

- When upgrades to product components, such as the scanning engine, are scheduled to end or will end within 30 days.
- When updates to detection definition (DAT) files have ended or will end within 30 days.

Task

For option definitions, click **?** in the interface.

1. In the SecurityCenter, click the **Policies** tab, then click **Add Policy** (or click **Edit** to modify an existing policy).
2. Click **Client Settings**.
3. On the Client Settings tab, under Display Settings, select or deselect **Display support notifications**.
4. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Configuring what users see

Use this task to select which components of the client software are displayed on client computers.

Task

For option definitions, click **?** in the interface.

1. In the SecurityCenter, click the **Policies** tab, then click **Add Policy** (or click **Edit** to modify an existing policy).
2. Click **Client Settings**.
3. On the Client Settings tab, under Display Settings, select an option for **Console display on client computers**.
   - **Show full console** — All client software options are displayed.
   - **Show status summary only** — The tray icon and menu are displayed, and users can open the console to display only the status of protection features on their computer.
   - **Show the icon only** — The tray icon is displayed, and the tray menu lists only the **Update Now** option.
4. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Uninstalling the client software

Use this task at a client computer to remove the Total Protection Service software. You might need to do this for testing purposes or before reinstalling the client software. (Note that not all types of protection include a client software component.)

NOTE: If you uninstall the client software, the computer is no longer protected. We recommend that you reinstall as soon as possible.

Task

1. Close the Microsoft Outlook and Internet Explorer applications.
2. In the Windows Control Panel, open **Add/Remove Programs**.
3. Select the types of protection you want to uninstall, then click **Remove**.
   - **McAfee Virus and Spyware Protection**
   - **McAfee Firewall Protection**
   - **McAfee Browser Protection**

   NOTE: On computers running the Windows firewall, the setting for the Windows firewall is automatically restored to the setting that was in effect before Total Protection Service firewall protection was installed. If the Windows firewall was enabled then, it is re-enabled automatically now.

Frequently asked questions

Why does the online help not display correctly?

If the built-in help system displays incorrectly on a client computer, its version of Microsoft Internet Explorer might not be using ActiveX controls properly. These controls are required to display the help file. Make sure that you install the latest version of Internet Explorer with its Internet security settings set to **Medium** or **Medium-high**.

I use Windows XP Service Pack 2, and I get a message that my computer may be at risk. What does this mean?

This is a known problem with Microsoft Security Center, because Microsoft cannot determine that Total Protection Service is installed and up-to-date. If you get this message when starting your computer, click the message balloon to open the Recommendation window, select **I have an antivirus program that I'll monitor myself**, then click **OK**.

Can computers using proxy servers receive updates?

If client computers are connected to the Internet by a proxy server, you might need to provide additional information for updates to work properly. Authentication support is limited to anonymous authentication or Windows domain challenge/response authentication. Basic authentication is not supported. Automatic updates do not occur when a CHAP or NTML proxy is set up in Internet Explorer.

Is it okay to delete the Temp folder in my program's directory structure?

No. Updates might fail if the Temp folder does not exist. If you delete the folder inadvertently, restart the computer to re-create the folder automatically, or manually create a Temp folder in the Program Files\McAfee\Managed VirusScan folder.

During an update, I get a message that one or more Total Protection Service windows are open, but I don't see any windows open. What should I do?

This occurs when a task that cannot be stopped, such as a scheduled scan, is running in the background. Wait for the task to complete, or restart the computer to proceed with the update.

Error messages

This section describes error messages that are related to using the Total Protection Service client features.

Unable to connect to Total Protection Service update server. Failed to connect to server for updates.

This error can be caused by several problems, but the most common solutions are:

- Check your connection to the network server or Internet.
- Empty the Internet Explorer cache and adjust the security level settings to **Medium** or **Medium-high**.
- Empty the Internet Explorer cache. (See your browser's documentation for instructions.)
- Adjust your corporate firewall or proxy settings.

Update failed.

There are several reasons that updates might fail.

- Check your connection to the network server or Internet.
- When using the Windows fast user switching feature, automatic updates cannot occur when no user is logged on if the computer is a domain controller or local security policies prevent the creation of a pseudo user.
- Automatic updates cannot occur on computers that are behind an authenticating proxy server or on computers where a CHAP or NTML proxy is set up in Internet Explorer.
- Automatic updates cannot occur where no user is logged on to computers that receive updates through a relay server.
- Updates might fail if the Temp folder does not exist on the client computer. If you delete the folder inadvertently, restart the computer to re-create the folder automatically, or manually create a Temp folder in the Program Files\McAfee\Managed VirusScan folder.

Activate your software.

You have not activated your copy of Total Protection Service. You cannot receive updates against the latest threats until you activate. To activate, click the Total Protection Service icon in the system tray, then select **Activate**.

Your software is not up-to-date. Please activate to receive the latest update.

You have not activated your copy of Total Protection Service. You cannot receive updates against the latest threats until you activate. To activate, click the Total Protection Service icon in the system tray, then select **Activate**.

Your subscription has expired. Your trial has expired. Renew your subscription to re-activate your software. Purchase a subscription to re-activate your software.

If you are using a pre-installed copy of Total Protection Service, your activated trial or your pre-installed subscription has expired. To activate, click the Total Protection Service icon in the system tray, then select **Buy** or **Renew your subscription**.

Using the SecurityCenter

Total Protection Service is designed for hands-off management. After installing the software on client computers, you receive regular emails that summarize the security status of all client computers on your account, and notify you of actions required to address vulnerabilities. Status emails contain a link to your McAfee SecurityCenter website, where you can view detailed reports and instructions for resolving problems.

In small organizations, status emails might be all that is needed to assure you that your computers are safe. If you manage a large account or want more proactive, hands-on involvement, you can take advantage of the management console available on the SecurityCenter.

Use the SecurityCenter to centrally manage the client computers and information for your account.

Contents

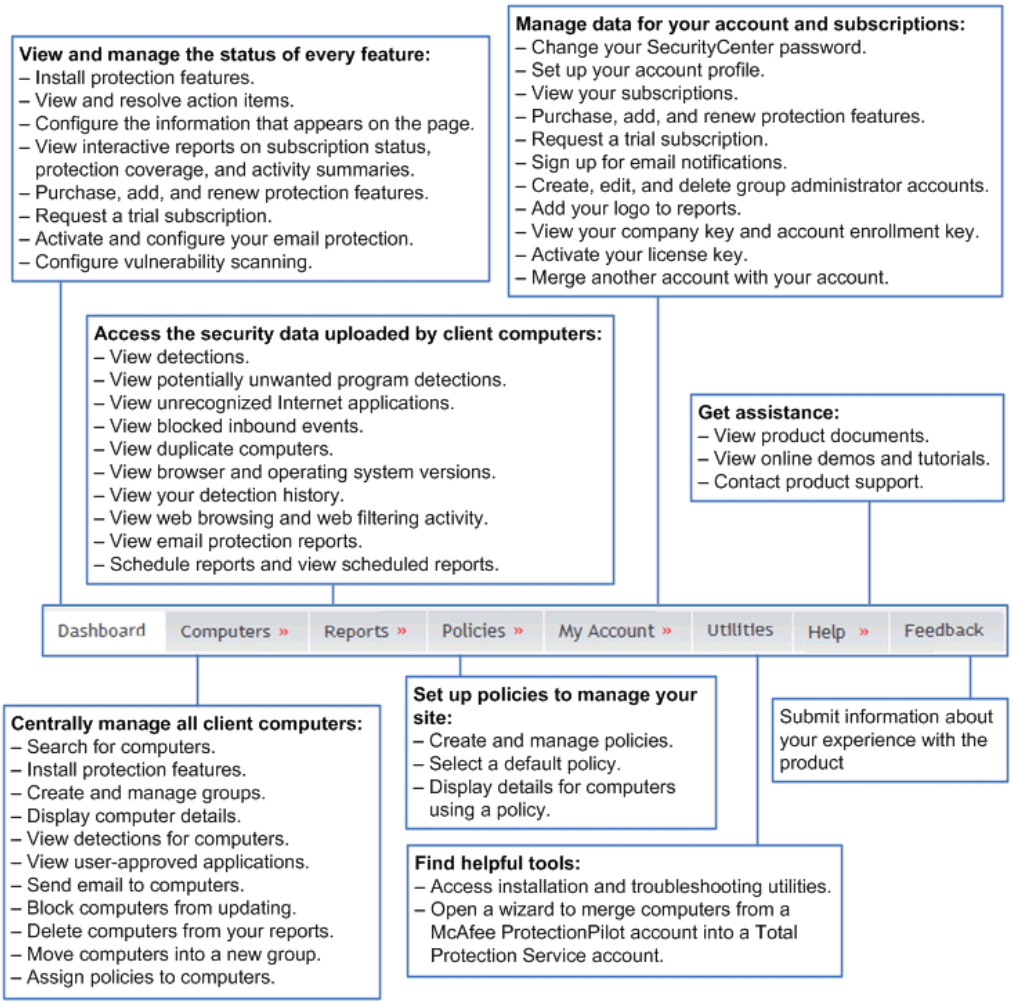
- The SecurityCenter
- Protection status at a glance
- Management of client computers
- Management of computer groups
- Management of Active Directory groups
- Management of group administrators
- Management of security policies
- Generation of security reports
- Managing your account
- Downloading tools and utilities
- Getting assistance
- Frequently asked questions about the SecurityCenter

The SecurityCenter

The SecurityCenter offers a management console for monitoring the protection status of computers on your account and assessing their security needs. Administrative features are divided among eight pages:

- Dashboard
- Computers
- Reports
- Policies
- My Account

- Utilities
- Help
- Feedback



Logging on to the SecurityCenter

Use this task to log on to the SecurityCenter and access administrative features.

Before you begin

Obtain the URL for your SecurityCenter in the login credentials email or weekly status email you received from your service provider.

NOTE: Before typing your login credentials, you can access multimedia demos and tutorials for more information about using the SecurityCenter. (Not available for all accounts.)

Task

1 Paste or type the URL into your browser.

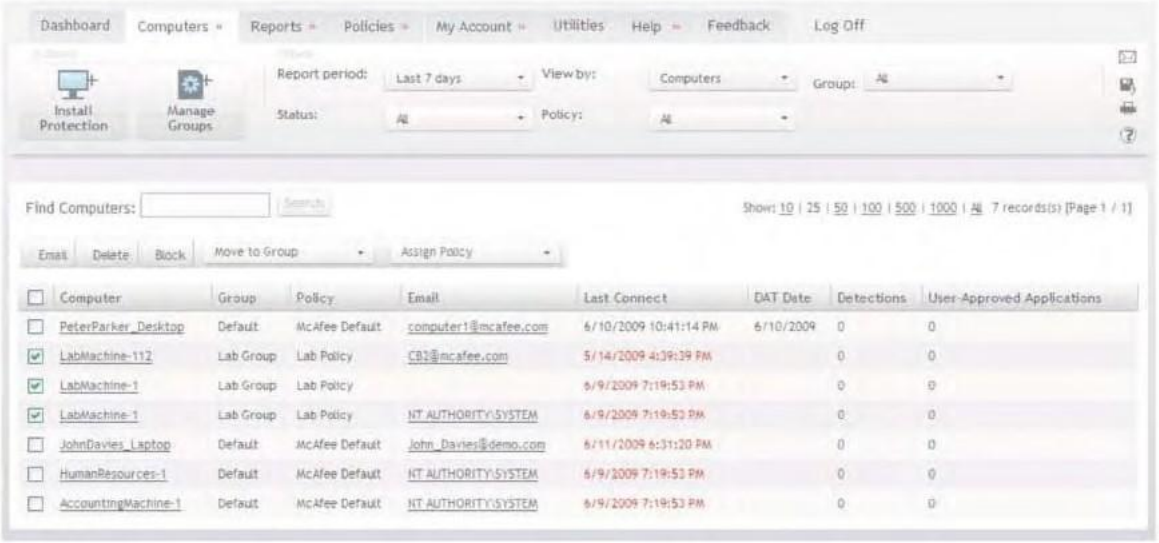
2 Type your login credentials.
- **Email address**: The email address that you used to sign up for Total Protection Service.

- **Password**: In most cases, the password that you created when signing up. If you have forgotten your password, click the link and it will be emailed to you at the login email address.

3 Click **Log On**.

Accessing data on SecurityCenter pages

Each SecurityCenter page includes features for displaying the exact data you need and using it efficiently.



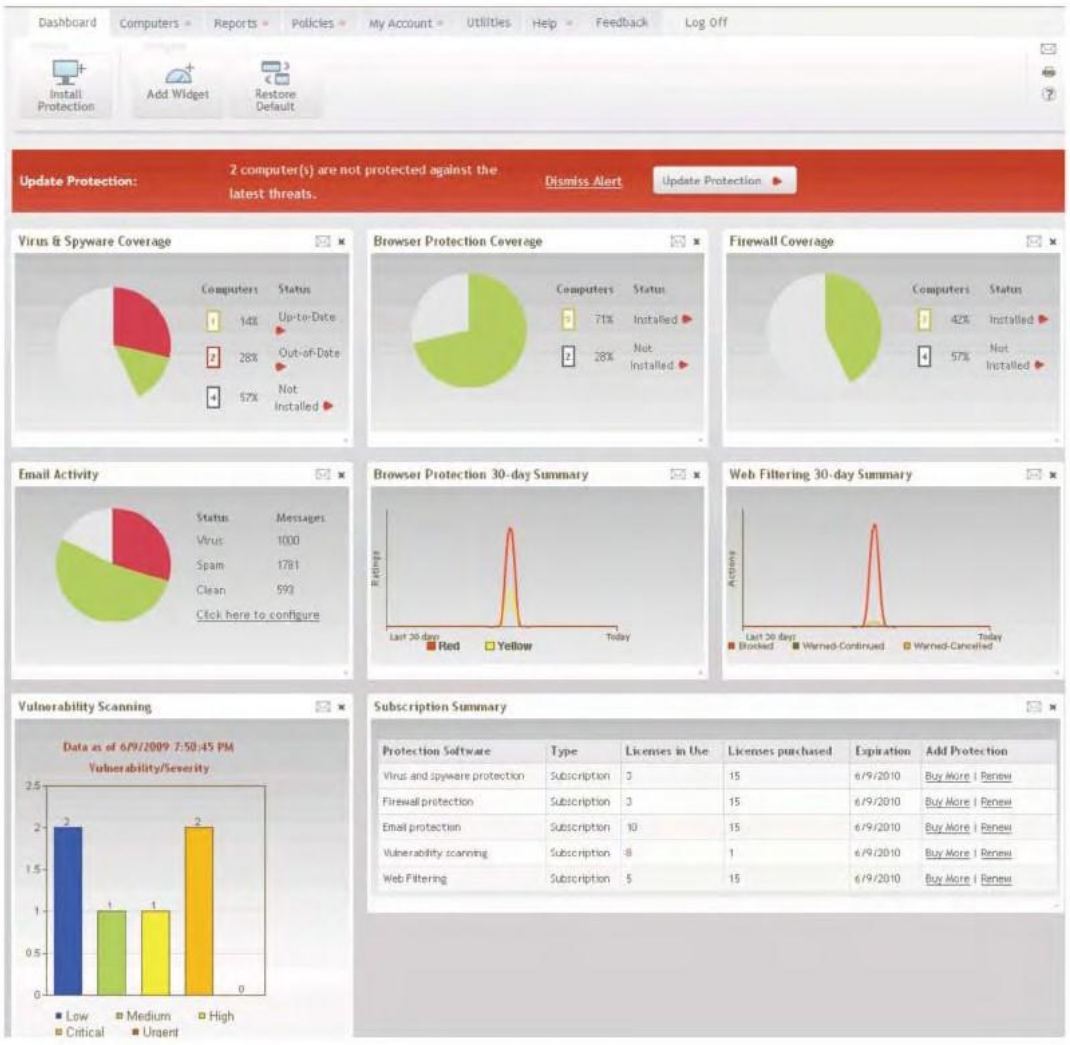
When you want to...	Do this...
Send the current page as an email attachment or scheduled report	Click the email icon (located along the upper-right margin of the page) to open the Scheduled Reports page, which contains a blank email message to fill out and delivery options. You can configure the message to be sent immediately or at regular intervals, then click **Save**. (You must have a local email application installed to use this feature.)
Print the current page	Click the print icon (located along the upper-right margin of the page) to open the page in a separate browser window, then select **Send to Printer** to open the Windows Print dialog box.
Save the current page as a file	Click the save icon (located along the upper-right margin of the page), then select the file format: • Microsoft Excel • Microsoft Word • Adobe PDF • Comma-separated text
Display context-sensitive help	Click the help (**?**) icon (located along the upper-right margin of the page) to display help for the current page, with links to related topics.
Navigate in multiple-page listings	Click the number of entries to display, or select a page number from the **Go to page** drop-down list.
Select computers to manage	Select the checkbox for individual computers, or select the checkbox in the heading to select all computers.

When you want to...	Do this...
Check your action items and alerts	Problems that require your attention appear in red. The method for resolving them varies depending on the page. • Click the button at the end of the text to display instructions for resolving the problem. • In a computer listing, click the name of the computer to display details about it, then click the action item.
Display details about a computer	Click a computer name in a listing.
Send email to a computer	Click an email address in the listing to open a blank, preaddressed message. (You must have a local email application installed to use this feature.)
Filter information on a page	At the top of a page, select the information to display (such as group name, period of time, or type of information). TIP: For greater flexibility in managing large accounts, select whether to display groups or individual computers.
Sort information in listings	Click a column heading to sort by that column. Click it again to switch the order in which it is displayed (ascending order or descending order).

Protection status at a glance

The **Dashboard** page is your "home" page on the SecurityCenter website — a graphical overview of your coverage with instant access to summary information about the computers and subscriptions in your account. Access the Dashboard page at any time by clicking the **Dashboard** tab.

- Install additional protection.
- View and resolve action items.
- View protection coverage and activity for all computers or specific groups with interactive reports (known as widgets) containing clickable charts and links.
- Check and update your subscriptions and licenses.
- Select, resize, and reposition the widgets that appear on the page.
- Access associated protection portals by clicking a link (available only when your account includes email protection or vulnerability scanning).



Viewing protection at a glance

Use this task to view details about your account and protection coverage, resolve action items, and update protection.

Task

For option definitions, click **?** in the interface.

1 Click the **Dashboard** tab.

2 Select the group for which you want to display information. *(Optional)*

3 Do any of the following:

To...	Do this...
View instructions to resolve an action item	Click the button at the end of the text. Action items are security issues that need your immediate attention.

To...	Do this...
Install additional protection	Click **Install Protection** to open a wizard that guides you through the steps for installing protection on new or existing computers.
Add clickable charts and graphs (widgets) to the page	Click **Add Widget**, select a chart or graph, then click **Add to Dashboard**.
Redisplay the default page configuration	Click **Restore Defaults**.
View details about protection coverage	In a widget, click a color in the pie chart that shows the status of client computers in your account. • Red — Out-of-date or unprotected systems. • Green — Up-to-date or protected systems. • Gray — Computers where protection is not installed.
Update protection	In the Subscription Summary widget, click **Buy**, **Buy More**, or **Renew**, then follow the instructions on the Product Purchase page.
Create trial subscriptions	Click the **Try** link in the Subscription Summary widget, or in a widget for a type of protection not included in your account.
Customize the appearance of the page	• To remove a widget, click its close box (in the upper-right corner). • To reposition a widget, click its title bar and drag it to a new location. • To resize a widget, click its border and drag to a new size. • To email the information in the widget, click the email icon (in the upper-right corner). You can also schedule it to be sent as an email attachment at regular intervals.

Working with widgets

Use this task to view, manage, and access information in widgets. Widgets are small, interactive reports that appear on the Dashboard page of the SecurityCenter. They provide summary and overview information about your account's protection status, activity, and subscriptions. Some widgets provide links to associated portals or subscription-related tasks.

You can add new widgets, remove widgets, and customize the way widgets appear.

Task

For option definitions, click **?** in the interface.

1 Click the **Dashboard** tab.

2 Do any of the following:

To...	Do this...
View details about protection coverage	In a widget, click a color in the pie chart that shows the status of client computers in your account.

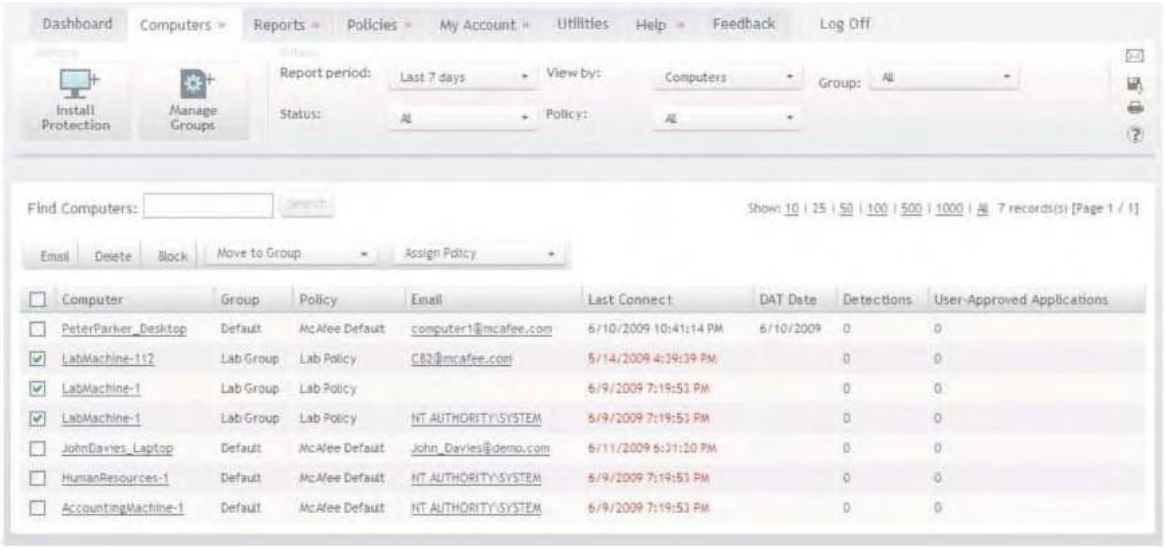
To...	Do this...
	• Red — Out-of-date or unprotected systems. • Green — Up-to-date or protected systems. • Gray — Computers where protection is not installed.
View details about activity	In a widget, click links that display more information about reported activity, such as the computer names or the number of detections.
Buy or renew subscriptions and licenses	Click links in the Subscription Summary widget.
Create trial subscriptions	Click the **Try** link in the Subscription Summary widget, or click a link in a widget for a type of protection not included in your account.
Open a protection portal in a separate browser window	Click the **Click here to configure** link in an email protection or vulnerability scanning widget. (Available only when your subscription includes these types of protection.)
Remove a widget	Click its close box (in the upper-right corner).
Reposition a widget	Click its title bar and drag it to a new location.
Resize a widget	Click its border and drag to a new size. (Two sizes are available.)
Email the information in the widget	Click the email icon (in the upper-right corner), then select delivery options to send it now or schedule it to be sent at regular intervals. (You must have a local email application installed to use this feature.)
Add widgets to the page	Click **Add Widget**, then for the widget you want to display click **Add to Dashboard**.

Management of client computers

The SecurityCenter provides a centralized location for working with all the computers in your account. You can instantly view each computer's group and email address, when it last connected to the network, whether its detection definition (DAT) file is current, the number of detections, and the number of Internet applications approved by its user. You can easily see which computers need your attention, display additional information, and perform necessary management tasks

Click the **Computers** tab to display the Computers page, which lists all the computers or groups in your account or only the computers in a selected group.

NOTE: The Computers page lists up to 5000 computers. For larger accounts, we recommend organizing your computers into groups of no more than 100 computers to optimize SecurityCenter performance.



From the Computers page you can click a computer name to display details of the individual computer on the **Computer Details** page.

Working with computers

Use this task to manage client computers from the Computers page.

Task

For option definitions, click **?** in the interface.

1. Click the **Computers** tab.
2. Select information filters to determine what you want to appear at the bottom of the page:
   - **Report period** — Specify the length of time for which to display information.
   - **View by** — Display individual computers or groups.
   - **Group** — Display only the computers in a group or display all computers. (Not available if you selected View by | Groups.)
   - **Status** — Show all computers, out-of-date computers, computers with detections, or computers you have blocked from receiving updates.
   - **Policy** — Show all computers or only those assigned a particular policy.
3. On the Computers page, do any of the following:

To...	Do this...
Find one or more computers	Type the full or partial name of a computer in the **Find Computers** box and click **Search**. NOTE: The computer search feature does not recognize wildcard characters, so type letters or numbers only. Site administrators can search the entire account; group

To...	Do this...
	administrators can search only the groups their site administrator has assigned to them.
Add one or more computers	Click **Install Protection** to open the install wizard, which guides you through the steps for installing protection on new or existing computers.
View or edit details for a computer	Click a computer name to display the Computer Details page for that computer.
Send email to users about their computer's problems or tasks they need to perform	Click an email address for a computer. Alternatively, select the checkbox for multiple computers in the list, then click the **Email** button. A blank preaddressed email message appears. (You must have a local email application installed to use this feature.)
Delete obsolete or duplicate computers from the listing	Select the checkbox for one or more computers in the list, then click **Delete**. NOTE: Deleting a computer does not remove the Total Protection Service client software. If you mistakenly delete a computer with enabled client software from the listing, it automatically reappears the next time its report data is uploaded; however, you can no longer view its historical detection data.
Block unauthorized computers from receiving updates	Select the checkbox for one or more computers in the list, then click **Block**.
Unblock computers from receiving updates	Select **Computer status | Blocked** to list all blocked computers, then select the checkbox for one or more computers and click **Unblock**.
Move computers into a group	Select the checkbox for one or more computers in the list, then select an existing group from the **Move to Group** list.
Assign a policy to computers	Select the checkbox for one or more computers in the list, then select an existing policy from the **Policy** list.
View detections for a computer	Click a quantity under **Detections** to open the Detections List, then click a detection name to view detailed information from the McAfee Avert® Labs Threat Library.
Add user-approved applications to one or more policies	**1** Click a quantity under **User-Approved Applications**. **2** In the User-Approved Applications List, click **Allow**, select the policies to add the approved applications to, then click **Save**. NOTE: The User-Approved Applications List shows detected programs that users have approved to run on the computer. To prevent users from approving applications, configure policy options for Protect mode.

Working with an individual computer

Use this task to manage an individual computer on the **Computer Details** page. This page displays information about the computer, its service components, and its detections.

Task

For option definitions, click **?** in the interface.

1 From a computer listing, such as the Computers page, click a computer name.

2 On the Computer Details page, do any of the following:

To...	Do this...
Update the email address	In the **System email address** box, type a new email address, then click **Save**.
Move the computer to a new group	In the Group list, select a group, then click **Save**.
Assign a new policy	In the Policy list, select a new policy, then click **Save**.
Install protection on an unprotected computer	Select the **Click here to install** link to open the installation wizard.
Display instructions for resolving an action item	Under Action Items, click the action item.
Display details about detections	In the Detections section, click a quantity under **Detections** or **User-Approved Applications** to display a detailed listing.
Add user-approved applications to one or more policies	**1** In the Detections section, click a quantity under **User-Approved Applications**. **2** In the User-Approved Applications List, click **Allow**, select the policies to add the approved applications to, then click **Save**. NOTE: The User-Approved Applications List shows detected programs that users have approved to run on the computer. To prevent users from approving applications, configure policy options for Protect mode.
View attempted visits to blocked websites	In the Detections section, click a quantity under **Blocked Sites** to open a page that lists details about each attempted visit. NOTE: This feature is available only when web browsing policy options are enabled in versions of Total Protection Service that include the web browsing module.

Management of computer groups

A group consists of one or more computers that share a particular feature. You can base groups on geographic location, department, computer type, the tasks performed by the users, or anything meaningful to your organization.

By default, every computer in your account is placed into a group called Default Group. You can create other groups to place them in instead.

Why use groups?

Groups help you manage large numbers of computers or computers that use different security settings (defined in policies). Groups are particularly helpful in larger organizations or companies that are widely distributed geographically. Placing similar computers into a single group enables you to view and manage security issues for the group separately from the other computers in your account.

For example, you might place all laptops used by traveling sales representatives into a single group called Sales Team. Then you can configure special security settings for those computers to provide greater protection against threats in unsecured networks such as airports and hotels. You can also track the number of detections on those computers through more frequent reports and adjust the security settings as needed.

Tips for large accounts

To more efficiently monitor large accounts and optimize SecurityCenter performance, we recommend that you organize your computers into groups of no more than 100 computers. This enables you to use the View filter to display reports and computer status by group, then drill down to see the individual computers within a group as needed.

How can I manage groups?

The **Manage Groups** page displays the groups in your organization. Access the page by clicking the **Manage Groups** button on the Computers page. If you have not created any groups or policies, only the Default Group is displayed.

The Default Group

Until you create additional groups, all computers are assigned to the Default Group when the Total Protection Service client software is installed. If you delete a group that contains computers, they are moved into the Default Group. You cannot change the name of the Default Group.

After you create additional groups, you can assign computers to them during the installation process or move computers into them at a later time.

Working with groups

Use this task to view and configure groups for your account.

Task

For option definitions, click **?** in the interface.

1 Click the **Computers** tab, then click **Manage Groups**.

2 On the Manage Groups page, do any of the following:

To...	Do this...
Create a group	**1** Click **Add Group**. **2** Type a name for the group. **3** Select the computers to add to the group. **4** Click **Save**.
View computers in a group	Under Computers, click a number to display the Computers page showing all the computers in the group.
Rename a group	Under Action, select **Rename**, specify a new name for the existing group, then click **Save**.

To...	Do this...
Delete a group	Under Action, select **Delete**, then click **OK**. NOTE: You cannot delete the Default Group. If you delete a group that contains computers, they will be moved into the Default Group.

Management of Active Directory groups

If you use Active Directory to define group hierarchies in your network, you can import the organizational unit (OU) structure into the SecurityCenter.

1. Download the Active Directory Synchronization utility.
2. Run the utility to import Active Directory groups from your network.
3. Install the client software on computers in your Active Directory groups. You can select a policy to assign during the installation process.
   - Create and send an installation URL to users to install on their computers.
   - Run a utility to "push" the software to multiple computers directly from the service provider's website.
4. Schedule a time for the Active Directory Synchronization utility to run on a regular basis to import any modifications made to the network Active Directory structure. This ensures that the information in the SecurityCenter stays up-to-date.
5. Check the status of the last synchronization tasks.

Your account can contain both Active Directory groups and groups that you create in the SecurityCenter.

See also

Management of computer groups on page 39

Downloading the Active Directory synchronization utility

Use this task to download a utility that imports Active Directory groups from your network into the SecurityCenter.

Run this task on an administrative computer that has a connection to an Active Directory server.

Task

For option definitions, click **?** in the interface.

1. On the Utilities page, click the **Active Directory Synchronization** tab.
2. Click **Download.**

Importing Active Directory groups

Use this task to import Active Directory groups from your network into the SecurityCenter.

Before you begin

You must download the Active Directory synchronization utility before you can perform this task.

Perform this task at an administrative computer has the client software installed and a connection to the Active Directory server.

Task

For option definitions, click **?** in the interface.

1. Click the product icon in the system tray, then select **Open Console**.
2. From the Action menu, select **Product Details**.
3. In the client console, select **Synchronize Active Directory**.
4. Enter your Active Directory credentials, the name and port for the Active Directory server, and your credentials for logging in to the SecurityCenter, then click **Log On**.
   The utility establishes a connection with the SecurityCenter and the Active Directory server.
5. Select the **Remember my credentials** option.
   This allows the utility to access the information on the Active Directory server the next time it runs. This option must be enabled for the utility to run on a scheduled basis to keep the information on the SecurityCenter up-to-date.
6. Select the groups to import, then click **Import**.
   You can select only the groups for which you entered credentials.
7. When the utility has finished importing your selection, click **Launch SecurityCenter** to proceed with installing client software.

Installing on Active Directory groups

Use this task to install the client software on computers in Active Directory groups.

Before you begin

You must import Active Directory groups before you can perform this task.

Note that all Active Directory organizational information is retained in the SecurityCenter. You cannot move Active Directory computers into groups that you have defined in the SecurityCenter, and no group selection options are displayed during the installation process.

Task

For option definitions, click **?** in the interface.

- In the SecurityCenter, select a method for installing the client software on the imported computers.
  - On the Dashboard page, click **Install Protection**, and follow the steps in the installation wizard for creating a URL to send to users. This allows them to install the software on their computers.
  - On the Utilities page, click the **Active Directory Configuration** tab, then under **Push Install utility** click **Download** to get a utility that "pushes" the software to multiple computers. Version 2.0 of the Microsoft .NET Framework redistributable package must be installed on the administrative computer to run the Push Install utility.

    When you run the Push Install utility, you select the Active Directory groups, the software to install, a policy to assign, and whether to scan the computer for threats when installation is complete. Click the help link (**?**) in the utility for online assistance.

Synchronizing Active Directory groups

Use this task to update the SecurityCenter with any modifications made to the Active Directory structure on the network by scheduling a synchronization utility.

The synchronization utility runs on a regular basis to keep the information synchronized automatically.

NOTE: In the utility, the **Remember my credentials** option must be selected for the utility to run on a scheduled basis. This allows the utility to access information on the Active Directory server.

Task

For option definitions, click **?** in the interface.

1. On the Utilities page, click the **Active Directory Synchronization** tab.
2. Under Synchronization Schedule, select **Enable scheduled synchronization**.
3. Select a day of the week or month to run.
4. If you want any groups that are part of the Active Directory structure on your network to be created in the SecurityCenter automatically, select **Allow group creation**. If you select this option, computers will be placed in the same groups they are in on your network. If you do not select this option, computers will be placed in the Default Group.
5. Click **Save**.

See also

Logging on as a site administrator on page 26

Viewing the synchronization status

Use this task to display details about the most recent activity to synchronize Active Directory groups in the SecurityCenter with your network.

Task

For option definitions, click **?** in the interface.

1. On the Utilities page, click the **Active Directory Synchronization** tab.
2. Under Synchronization Status, check the last time the synchronization utility ran.
3. Click **View synchronization history**.

A page lists up to 25 computers that ran the synchronization task and the results.

Viewing the Active Directory tree in the SecurityCenter

Use this task to view Active Directory computers and groups you have imported into the SecurityCenter.

Task

For option definitions, click **?** in the interface.

- Perform one of these tasks.
  - On the Utilities page, click the **Active Directory Synchronization** tab, then click **Active Directory Structure** to open a page showing the Active Directory tree for your account.

- On any page with a **Groups** filter, click the icon that appears to the right of the drop-down list to open a page where you can select computers or groups.
- On pages that display a group listing, click the viewing icon for the tree view. The viewing icons, which appear just above the left top corner of the group listing, select a flat listing of group paths and names or a tree view.

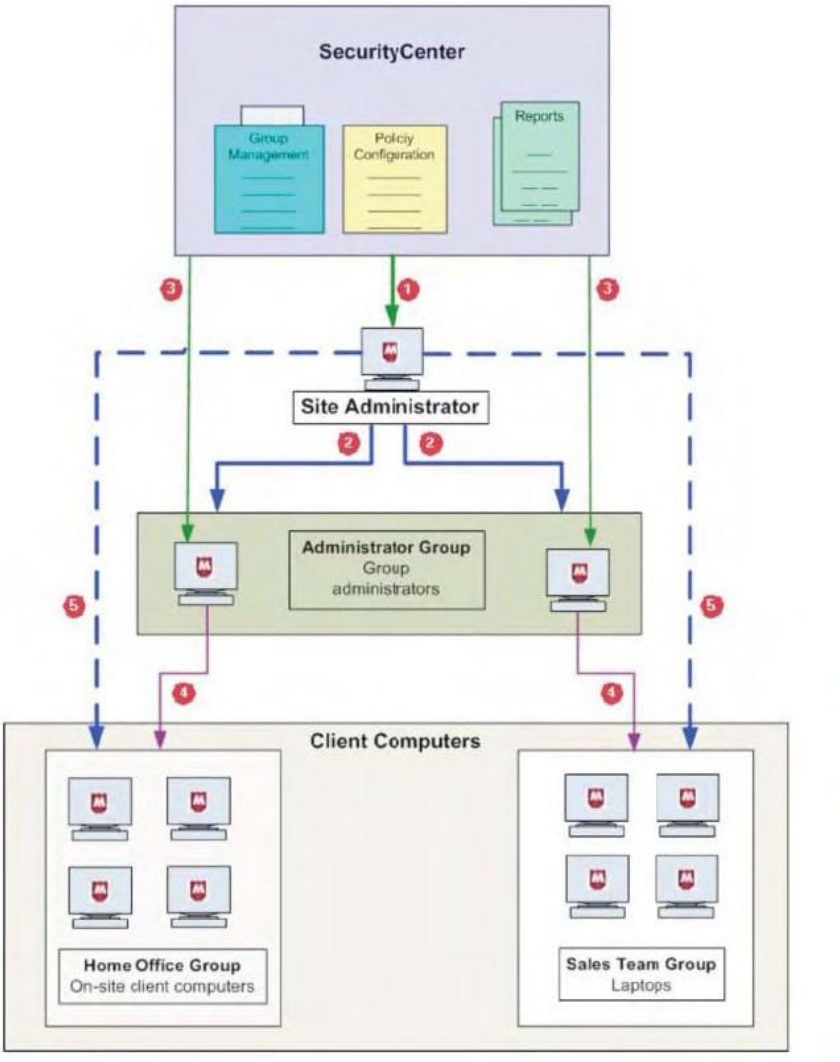
Management of group administrators

Group administrators oversee and manage the groups that you, the site administrator, assign to them. When creating group administrators, you specify which groups they manage, a password they use to access the SecurityCenter, and their access level.

Why use group administrators?

Create group administrators to distribute security management in large organizations

Group administrators have fewer access rights than the site administrator. While the site administrator can access all security information for all client computers in the account, group administrators can access information only for client computers in the groups they are assigned to.



1 The site administrator communicates directly with the SecurityCenter to create policies, check reports, and maintain the SecurityCenter account.
2 The site administrator creates and manages group administrators.
3 Group administrators communicate directly with the SecurityCenter to access security data for the groups they are assigned to.
4 Group administrators manage the client computers in their assigned groups. The management tasks they can perform and the information they can access on the SecurityCenter depend on the access level assigned to them.
5 The site administrator can manage all client computers in all groups.

What can group administrators do?

The access level you assign to group administrators determines which tasks they can perform for their groups. Select from two access levels:

- Read Only
- Read and Modify Reports

Basic tasks for Read Only	Additional tasks for Read and Modify Reports

• Access the SecurityCenter website.
NOTE: No subscription information is visible. Only the assigned groups are visible.
• Manage from client computers:
  • Manage quarantined files.
  • Disable on-access scanning.
  • View the status of a scheduled scan in progress.
• View computers from the SecurityCenter.
• Check data in reports.
	• Install protection.
	• View and manage computers from the SecurityCenter.
	• View policies.
	• Rename groups.
	• Modify the information in listings and reports:
	  • Send email to computers.
	  • Block computers from receiving updates.
	  • Delete computers from your reports.
	• Move computers in and out of groups.
	• Send email to users.
	• Schedule and send reports to users in email.

Working with group administrators

Use this task to manage group administrators on the My Account page. Here you can view, edit, create, or delete group administrators. Up to six group administrators can be listed. If you have created more than six group administrator accounts, click **View all group administrators** to display a complete listing.

Task

For option definitions, click **?** in the interface.

1 Click the **My Account** tab.
2 Click the **Group Administrators** tab, then do any of the following:

To...	Do this...
Add a group administrator	**1** In the Group Administrators section, select **Add**. **2** On the Manage Group Administrators page, select **Create New**. **3** Type the group administrator's name, email address, and password. **4** Select an access level. **5** For each group you want the administrator to manage, select the group in the listing on the left, then click **Add Group**. **6** Click **Save**.
Modify information for a group administrator	**1** Under Actions, select **Edit** for the group administrator you want to update. **2** On the Add Group Administrators page, modify information, then click **Save**.
Delete a group administrator	Under Actions, select **Delete** for the group administrator you want to delete, then click **OK**.
Email a new password to a group administrator	Under Actions, select **Email Password**. After your local email application opens a preaddressed message explaining how to log on to the SecurityCenter, assign groups, and access information about their responsibilities, send the email. NOTE: You must have a local email application installed to use this feature.

Management of security policies

Policies are made up of security settings for all of your protection features. These settings define how protection features operate on client computers.

Why use policies?

Policies enable you to customize security settings for your entire organization or for different computers in your organization. You can assign a unique policy to each computer or allow all computers to share a single policy.

For example, you might place all laptops used by traveling sales representatives into a single group called Sales Team. For each computer in the group, you can assign a policy with high security settings that will provide greater protection against threats in unsecured networks such as airports and hotels. Whenever you want to adjust those setting, simply change the policy. Your changes will be applied to all the computers in the Sales Team group automatically. There is no need to update each computer's setting individually.

How can I manage policies?

The **Policies** page displays all your policies. Use this page to create, copy, modify, and delete policies for your account. If you have not created any policies, only the McAfee Default policy is displayed.

McAfee Default policy

Until you create additional policies, all computers are assigned the McAfee Default policy, which is configured with settings recommended by McAfee to protect many environments and ensure that all computers can access important websites and applications until you have a chance to create a customized policy.

You cannot rename or modify the McAfee Default policy. When you add computers to your account, the McAfee Default policy is assigned to them. When you delete a policy that is assigned to one or more groups, the McAfee Default policy is assigned to those groups automatically.

The first time you create a new policy, the McAfee Default policy settings appear as a guideline. This enables you to configure only the settings you want to change without having to configure them all.

After you create one or more new policies, you can select a different default policy for your account. In the future, new policies will be prepopulated with these default settings, and the new default policy is assigned to new computers (if no other policy is selected) and groups whose policy is deleted.

NOTE: This section explains only the settings for the McAfee Default policy. See the chapters for particular types of protection for a complete explanation of all related policy options.

Client Settings

Option definitions — Client Settings Tab

Option	Definition
Update Settings	
Check for updates every	**12 hours**: Client computers check for updated detection definition (DAT) files and product components every 12 hours.
Update client computers where users are not logged in	**Disabled**: Automatic updates do not occur on computers where no user is logged on (for example, terminal servers and computers where the fast user switching feature is used). This prevents failed automatic updates that would be reported as errors.
Display Settings	
Console display on client computers	**Show full console**: Allow users to view the Total Protection Service icon and access all the client software features.
Hide the splash screen	**Disabled**: The McAfee Total Protection Service splash screen is displayed when a computer is powered on and the client software starts running.
Display support notifications on client computers	**Enabled**: Notification dialog boxes warn client computer users when software upgrades and DAT file updates are being discontinued for their operating system.

Virus and Spyware Protection

No excluded files and folders or approved programs are configured.

NOTE: With the default advanced settings for virus and spyware protection, it is possible for an on-demand scan to detect threats in archived files that are not detected during an on-access scan. This is because on-access scans do not look at compressed archives by default. If this is a concern for your organization, you should create a new policy where this option is enabled.

Option Definitions — General Settings Tab

Option	Definition
Scheduled Scan Settings	**Off**: No on-demand scan is scheduled. On-access scans still occur every time users run, open, or download files.
Spyware Protection Mode	**Prompt**: Spyware scanning is enabled. When potentially unwanted programs are detected, virus and spyware protection asks users how to respond. NOTE: To prevent prompts from displaying, create a new policy with a different setting. For maximum protection, we recommend selecting Protect mode to automatically delete potentially unwanted programs.

Option Definitions — Advanced Settings Tab

Option	Definition
Virus Protection Settings	
Enable outbreak response	**Enabled**: Client computers check for an outbreak detection definition (DAT) file every hour.
Enable buffer overflow protection	**Enabled**: Detect code starting to run from data in reserved memory and prevent that code from running.
Enable script scanning	**Enabled**: Detect harmful code embedded in web pages that would cause unauthorized programs to run on client computers.
Scan email (before delivering to the Outlook Inbox)	**Enabled**: Look for threats in email before it is placed into the user's Inbox.
Scan all file types during on-access scans	**Enabled**: Look for threats in all types of files, instead of only default types, when they are downloaded, opened, or run. (Default file types are defined in the DAT files.).
Scan within archives during on-access scans (e.g., .zip, .rar, .tat, .tgz)	**Disabled**: Do not look for threats in compressed archive files when the files are accessed.
Scan within archives during on-demand scans (e.g., .zip, .rar, .tat, .tgz)	**Enabled**: Look for threats in compressed archive files when files are scanned manually and during scheduled scans.
Enable Artemis heuristic network check for suspicious files	**Enabled**: Send information about unrecognized threat detections to McAfee Avert Labs for analysis.
Scan mapped network drives during on-access scans	**Disabled**: Do not look for threats in files on mapped network drives when they are accessed.
Enable on-access scanning (if disabled) the next time client computers check for an update	**Enabled**: If on-access scanning is disabled on a client computer, it is re-enabled when the computer checks for updates.
Maximum percentage of CPU time allocated for on-demand and scheduled scans	**High**: These scans are allowed to use a high percentage of CPU time. (Scans should be requested during non-peak hours, when users are not performing tasks on their computers.)
Spyware Protection Settings	
Detect ...	**Enabled**: Detect all types of spyware threats during scans.

Firewall Protection

No allowed applications are configured.

Option definitions — General Settings Tab

Option	Definition
Firewall Configuration	**User configures firewall**: Users must configure firewall protection for their computers. When this option is selected, other firewall protection options do not appear on this page. NOTE: It is important to educate users about threats and strategies for avoiding intrusions. To ensure the highest level of security, we recommend that administrators create a new policy and configure firewall protection.

Browser Protection

Option definitions — General Settings

Option	Definition
Automatically install browser protection on all computers using this policy	**Disabled**: Do not check whether browser protection is installed on computers checking for updates. (This option is available for all versions of Total Protection Service.)

Browser Protection & Web Filtering

No exceptions or content rules are configured.

Web Filtering options appear only in versions of Total Protection Service that include the web browsing module.

Option definitions — General Settings

Option	Definition
Automatically install browser protection on all computers using this policy	**Disabled**: Do not check whether browser protection is installed on computers checking for updates. (This option is available for all versions of Total Protection Service.)
Access to Sites	Regulate access to websites according to their safety ratings: • Yellow: Warn • Red: Block • Unrated: Allow
Access to Downloads	Regulate access to file downloads according to their safety ratings: • Yellow: Warn • Red: Block • Unrated: Allow NOTE: This feature is not supported on Firefox browsers.
Block phishing pages	**Enabled**: Do not allow access to pages with phishing content, even if they are located on a website with a green overall safety rating.
Enforcement Messaging	Display this message when users attempt to access blocked content: • **Language**: The default language for your account. • **Message**: **An unacceptable security risk is posed by this site.**
Browser Protection Status	
Disable browser protection on all computers using this policy	**Disabled**: Do not disable browser protection on computers using this policy.
Allow users to enable or disable browser protection	**Disabled**: Do not allow browser protection to be disabled at the client computer.

Working with policies

Use this task to create and modify policies from the **Policies** page. You can also select a new default policy for your account.

Task

For option definitions, click **?** in the interface.

1 Click the **Policies** tab.

2 On the Policies page, do any of the following:

To...	Do this...
Specify a default policy	Select an existing policy from the Default Policy list.
Create a policy	**1** Click **Add Policy**. NOTE: The new policy is prepopulated with settings from the McAfee Default policy or another policy that you have selected as the default for your account. To prepopulate a new policy with settings from a different policy, locate the policy and select **Copy**. **2** Type a name for the policy. **3** Configure the settings on each tab. **4** Click **Next**. **5** Assign the policy to one or more computers or groups. *(Optional)* **6** Click **Save**.
Edit a policy	**1** Under Actions, select **Edit** for the policy. **2** Make changes to the policy, then click **Save**.
Delete a policy	Under Actions, select **Delete** for the policy, then click **Save**. NOTE: If you delete a policy that is assigned to one or more groups, the default policy you have selected for your account (or the McAfee Default policy) is assigned to the groups in its place. You cannot delete the McAfee Default policy.

Generation of security reports

Whenever a client computer checks for updates, it also sends its scanning history, update status, and detections to the SecurityCenter website in encrypted XML files. It uploads the data directly through an Internet connection or via a relay server. Report data is saved for one year.

To view this data, click the **Reports** tab to display the Reports page. You can display reports that include all the computers on your account (using the same company key) or only computers in a particular group.

Why use reports?

Reports provide valuable tools for monitoring detections and fine-tuning your protection strategy. Only the reports available for the types of protection installed appear on this page.

Emailing and scheduling reports

You can run reports on demand or schedule them to at run regular intervals and then send them as email attachments to one or more recipients.

NOTE: For more information about reports for specific types of protection, see the chapters for those types of protection. For versions of Total Protection Service that include vulnerability scanning, reports are available on the vulnerability scanning portal.

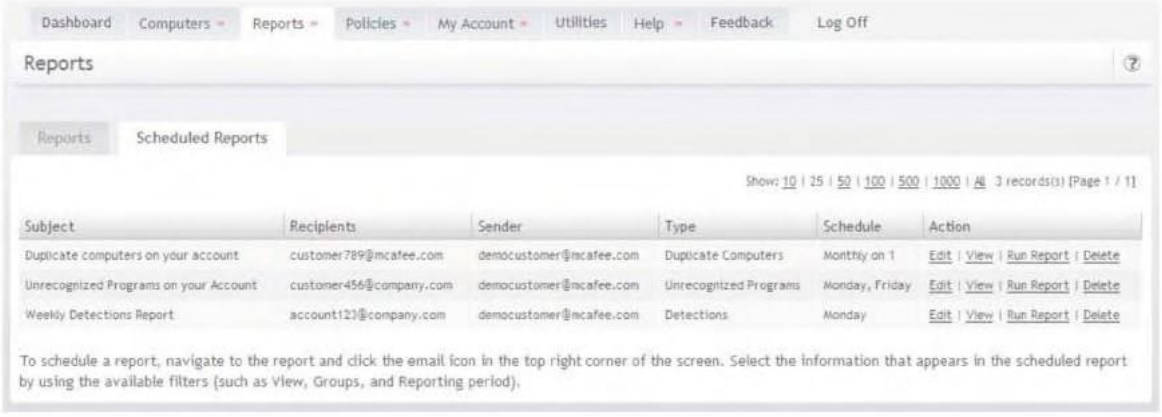
Use this report...	To view...
Detections	The types of potentially malicious code or unwanted programs that have been found on your network. Use this report to manage detections of viruses and potentially unwanted programs.
Unrecognized Programs	Programs that spyware protection or firewall protection detected on your network. Use this report to manage your potentially unwanted program detections and Internet applications blocked by firewall protection. You can add approved programs and allowed Internet applications to policies directly from the report.
Inbound Events Blocked by Firewall	Computers where inbound or outbound communications were blocked by firewall protection. Use this report to manage blocked communications. NOTE: For blocked events to be reported, the **Report blocked events** option must be enabled in the Firewall Protection policy. Blocked events are logged for all computers that are assigned a policy where this option is enabled.
Duplicate Computers	Computers that appear more than once in administrative reports. Use this report to track down obsolete computers and those where Total Protection Service has been incorrectly reinstalled and tracked as multiple installations.
Computer Profiles	For each client computer, the version of the Microsoft Windows operating system and Microsoft Internet Explorer web browser running, which group it belongs to, whether it is configured as a relay server, and other details. Use this report to locate computers where you need to install software patches for a specific browser or operating system, check the version of the client software, identify relay servers, and identify the group number for use in silent installation.
Detection History	A graphical summary of the number of detections and the number of computers where detections occurred on your network over the past year. Use this report to evaluate the effectiveness of your security strategy.
Web Filtering Report	A summary of browsing activity on your account. Shows the types of sites that client computers attempted to access by content rating and category. Includes successful, warned, and blocked access attempts. (Available only when web filtering policy options are

Use this report...	To view...
	enabled for versions of Total Protection Service that include the web filtering module.) Use this report to evaluate the types of sites being accessed by which computers and the effectiveness of the content rules defined in policies.
Email Protection Reports	A page on the email protection portal, where you can access reports on your site's mail flow and detections. (Available only for versions of Total Protection Service that include email protection.) Use these reports to monitor email activity and detections.

Scheduling reports

Use this task to send information from the SecurityCenter as an email attachment at regular intervals. This type of information can be scheduled:

- Reports
- Dashboard page
- Computers or Computer Details page
- Widgets on the Dashboard page



Task

For option definitions, click **?** in the interface.

1. Display the page or widget that shows the information you want to send.
2. Click the email icon in the upper-right corner. A blank email message appears.
3. Select delivery options.
   - **Immediately** — Send the information once, as soon as you click **Save**.
   - **Weekly on** — Send the information each week, on the selected day.
   - **Monthly on** — Send the information each month, on the selected day.
4. Type one or more email addresses to receive the report. Separate multiple addressees with commas.
5. Type a subject and a message for the email.
6. Click **Save**.

Adding your logo to reports

To customize your reports, you can upload a logo that appears in the upper-right corner of the SecurityCenter website and reports. Use this task to add or delete a logo.

Logo files can be .gif, .jpeg, .jpg, or .png format. Logo dimensions must be 175 x 65 pixels with a file size under 500 KB. Other dimensions will result in a stretched or shrunken logo.

Task

For option definitions, click **?** in the interface.

1 On the My Account page, click the **My Profile & Logo tab**. The My Logo section displays the current logo, or a placeholder if you have not uploaded a logo.

2 Click **Edit**.

3 On the Manage Logo page, perform a task.

To...	Do this...
Add or replace a logo	**1** Click **Upload New Logo**. **2** On the Upload Your Logo page, type the name of the file you want to upload or browse to locate the file. **3** In the Verification Code box, type the characters displayed in the black box. Alphabetic characters are not case-sensitive. **4** Click **Upload Logo**. If your logo file is not the correct size, the SecurityCenter resizes it to fit the allotted area and displays a preview of how it will appear on reports. • Click **Approve** to accept the resized logo. • Click **Delete and Resubmit** to select a different file. **5** Click **Close Window**.
Delete a logo	Click **Delete Logo**.

4 Click **Done**.

Computer Profiles report

Use this report to view the version of the Microsoft Windows operating system and the Microsoft Internet Explorer web browser running on client computers. This helps you locate computers for maintenance, such as installing Microsoft software patches.

This report also shows whether computers are configured as relay servers, group information, and the version of software and DAT files.

Select the information that appears in this report

Select this option...	To do this...
Operating system version	Specify computers running all Windows operating systems or only those running a selected version.
Browser version	Specify computers running all versions of Internet Explorer or only those running a selected version.

Select this option...	To do this...
Groups	Display all the computers on your account or only those in the selected group.

How to use this report

When you want to...	Do this...
Identify computers running an operating system that needs an update or patch installed	Filter the listing to display only computers running the specific operating system.
Identify computers running a browser that needs to be updated	Filter the listing to display only computers running the specific operating system.
Send email notifying users about issues or maintenance specific to their operating system or browser	Select the checkbox by appropriate computer, then click **Email** to open a blank message to fill in and send. (You must have a local email application installed to use this feature.)
Locate group information for computers	Check the name and number of the group for each computer. (The group number is the group ID required when using the silent installation method [VSSETUP] to install client software.)
See which computers are configured as relay servers	Check the Relay Server column.
Check details about the files running on computers	Check the version of the DAT file and the client computer software (agent build number).

Duplicate Computers report

Use this report to locate computers that are listed more than once in your reports. Duplicate listings usually result when the Total Protection Service client software has been installed more than once on a single computer or when users install it on their new computers without uninstalling it from their previous computers.

Select the information that appears in this report

Select this option...	To do this...
Groups	Display all the computers on your account or only those in a single group.

How to use this report

When you want to...	Do this...
Delete duplicate computers	Select the checkbox for each duplicate computer listed, then click **Delete**. NOTE: Deleting a computer does not remove the Total Protection Service client software. If you mistakenly delete a computer with enabled client software from the listing, it automatically reappears the next time its report data is uploaded; however, you can no longer view its historical detection data.
View details about a computer	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.

Managing your account

Use these tasks to manage your Total Protection Service account from the **My Account** page. Management tasks are divided among four tabs.

- **My Profile & Logo** — Update the contact information for your account and add a customized logo to appear in reports.
- **Subscription & Notification** — View details about your current and past subscriptions, buy or renew a subscription, buy more licenses, request a trial subscription, and select the automatic emails you want to receive.
- **Group Administrators** — Create and manage administrators for groups in your account.
- **Accounts & Keys** — View the company key, enrollment key, and license key for your account or merge another account into your account.

Tasks

► Configuring your account profile
► Signing up for email notifications
► Viewing and updating subscription information
► Buying and renewing subscriptions and licenses
► Locating or creating keys for your account
► Merging accounts

Configuring your account profile

Use this task to update information in your customer profile when it changes. Your profile contains the information your service provider needs to contact you about your account. Initially, information supplied during your product purchase is placed into your profile. It is important to keep this information up-to-date to prevent a disruption in your protection.

Task

For option definitions, click **?** in the interface.

1. On the My Account page, click the **My Profile & Logo** tab.
2. In the My Profile section, click **Edit**.
3. Type or select information as needed.
   - Your password for logging on to the SecurityCenter.
   - Your administrator email address.
   - Contact information.
   - Language for account correspondence and notifications.
4. Click **Save**.

Signing up for email notifications

Use this task to select the email notifications you want to receive from your service provider.

Task

For option definitions, click **?** in the interface.

1. On the My Account page, click the **Subscription & Notification** tab.
2. In the Notification Preferences section, click **Edit**.
3. Sign up for email notifications for account status and subscription expiration. The type of notifications available depends on your service provider.

   NOTE: Status emails keep you informed about detections and coverage for your account. It is important to receive status emails at regular intervals that are appropriate for your account, based on the frequency with which you need to review detection information. By default, you receive status emails weekly.
4. Click **Save**.

Viewing and updating subscription information

Use this task to view current and cancelled subscriptions and to update subscription information. It is important to check the status of your subscriptions to ensure that protection remains active and you have the right number of licenses to protect new computers as your organization grows.

Task

For option definitions, click **?** in the interface.

1. On the My Account page, click the **Subscription & Notification** tab. The Subscription Summary section lists details about each subscription, including the number of licenses and their expiration date.
2. Do any of the following.

To...	Do this...
Purchase or extend coverage	In the Subscription Summary section, check the number of licenses available and their expiration dates. If needed, click **Buy**, **Buy More**, or **Renew**.
View details of each subscription	Click **View subscription history**.
Update information for a subscription	**1** Click **Edit**. **2** On the Edit Subscription Information page, type new information for any of the following: • Email address • Company name • First name or Last name **3** Click **Submit**.
Display a list of subscriptions that are no longer current	Select **View cancelled subscriptions**.

Buying and renewing subscriptions and licenses

To ensure that additional or renewed services remain on the same account with your existing services, follow these guidelines:

- Submit your order through the same SecurityCenter account you use to maintain your original subscriptions.
- Submit your order with the same email address you use to log in to the SecurityCenter.

By keeping all your subscriptions on the same account, all your client computers report to the same SecurityCenter website, and your service provider sends all correspondence and notifications to one email address.

If you do purchase subscriptions on multiple accounts, you can merge them into a single account.

NOTE: You can configure your notification preferences to receive an email whenever the expiration date for a subscription approaches.

Use this task to buy, add, or renew subscriptions and licenses. Subscriptions entitle you to a certain type of protection (such as virus and spyware or web filtering) and the number of licenses determine how many computers are protected.

Task

1 On the My Account page, click the **Subscription & Notification** tab. The Subscription Summary section lists details about each subscription, including the number of licences and their expiration date.

2 In the Add Protection column, click **Buy**, **Buy More**, or **Renew**, as needed.

NOTE: To try a new type of protection free-of-charge for 30 days, request a trial subscription by clicking **Try**. Before it expires, you will have an opportunity to purchase the full subscription and continue using it with no interruption.

3 Follow the instructions on the Product Purchase page.

Locating or creating keys for your account

Use this task to reference these keys for your account:

- Company key — Required for URL-based or silent installation of client software.
- Account enrollment key — Required to activate pre-installed versions of client software and place them under your account. If no valid enrollment key exists, create a new one.

NOTE: A license key is required to activate CD-based versions of the client software. Locate the license key on the CD label. See the installation guide for activation instructions.

Task

For option definitions, click **?** in the interface.

1 On the My Account page, click the **Accounts & Keys** tab.

2 Do any of the following.

To...	Do this...
Access your company key	Locate the company key for your account in the Company Key section.
Install protection on new computers	• Click **standard URL installation** to open the installation wizard. • Click **VSSETUP** to download the silent installation utility. See the installation guide for more information.
Access your account enrollment key	Locate the enrollment key for your account in the Account Enrollment Key section
Create a new company key	Click **Create a new key**. Company keys are valid for seven days.

Merging accounts

Use this feature to merge other installations of Total Protection Service into your account. This is useful when the client software was installed using another license key or when licenses were purchased using another administrator's email address.

For example, if you set up Account 1, then order additional licenses and activate them with a different email address than the one you originally used, the new licenses appear in Account 2. To view all the computers and licenses under Account 1, you must merge Account 2 into Account 1.

Once they are merged, Account 2 no longer exists. All the computers and licenses formerly listed under Account 2 are listed in the SecurityCenter for Account 1.

Task

1 On the My Account page, click the **Accounts & Keys** tab.
2 In the Manage Accounts section, select **Merge another account**.
3 On the Step 1 page, enter the email address and password activated for the account you want to merge into your main account, then click **Next**.
4 On the Step 2 page, view details for the account you have selected. Verify that the licenses and computers listed for the account are the ones you want to merge, then click **Next**.
5 On the Step 3 page, click **Merge Account**.

Downloading tools and utilities

Use this task to access helpful tools for managing your Total Protection Service account.

NOTE: Information on using the utilities related to installation is available in the installation guide, available from the Help page.

Task

For option definitions, click **?** in the interface.

1 Click the **Utilities** tab.

2 Click a link to select one of these utilities.

- URL installation — Opens the wizard, which guides you through the steps for selecting which software to install on which computers. Select this option from a client computer.
- Silent installation — Downloads the silent installation package, which enables you to deploy Total Protection Service on a client computer with no user interaction. Select this option from either an administrative or client computer.
- Push Install utility — Runs an ActiveX control that enables you to deploy the client software directly from the service provider's server onto multiple client computers. Select this option from an administrative computer.
- Uninstall utility — Downloads a cleanup utility that removes components left from a previous installation of Total Protection Service or another vendor's protection software. Select this option from a client computer, then double-click to begin installation.
- Standalone installation agent — Downloads software that you can install on client computers to allow users without administrative rights to install the client software.
- McAfee ProtectionPilot Migration Assistant — Downloads a wizard that guides you through the steps for migrating computers in a McAfee ProtectionPilot account to a Total Protection Service account. A link to documentation is also provided.

Getting assistance

Use this task to get assistance in using Total Protection Service and the SecurityCenter.

Context-sensitive online help is available on any page of the SecurityCenter by clicking the help link (**?**) in the upper-right corner.

Task

- Click the **Help** tab, then do any of the following:

To...	Do this...
View online documents	Click a link for the *Product Guide*, *Installation Guide*, or *Release Notes*.
View demos and tutorials	Click the icon for a multimedia presentation. • **View the Total Protection Service Demo** — Describes how the product protects computers on your account. • **View the Installation Tutorial** — Describes how to install the product. • **View the SecurityCenter Demo** — Describes how to use the features of the administrative website to manage your account. NOTE: Your service provider determines which demos are available.
Contact product support	Click an option. • **Online support** — Opens a form where you can submit a description of your problem to a product support representative. • **Phone support** — Displays a phone number and the grant number for your subscription. You will need to reference the grant number when you speak to a support representative.

Frequently asked questions about the SecurityCenter

This section includes questions asked by administrators that are related to using the features of the SecurityCenter.

- Reporting
- Adding, renewing, and moving licenses

Questions about reporting

Why don't some of my computers show up on my reports?

If your company added more licenses, or upgraded from a trial to a full subscription, some computers might not appear in your reports.

If you upgraded or purchased additional protection using a new email address, you received a new company key and URL for a new account instead of adding licenses to your existing account. (The company key appears after the characters CK= in the URL. It also appears on the Account & Keys tab of the of the My Account page of the SecurityCenter.) Because you have two company keys, reports appear in two places. Make sure all your trial users reinstall with the installation URL associated with the new key. If you do need to merge multiple accounts, then use the Manage Accounts section of the Accounts & Keys tab.

Why do my cloned systems all report as the same computer?

The client software generates a unique system identifier when it is installed. If a drive is imaged after the software was installed, all the cloned systems have the same system identifier. To avoid this problem, the software must be installed after the new systems are restarted. You can do this automatically by using the silent installation method, described in the installation guide.

I just installed Total Protection Service and don't have much information on my SecurityCenter website. Can I view sample reports?

Yes. Sample reports are available at:

http://www.mcafeeasap.com/MarketingContent/Products/SampleReports.aspx

Sample reports are useful for new administrators who do not have many users or much detection data and, therefore, cannot view some advanced reporting features.

NOTE: Sample reports are available in all product languages. Select the language from the **Global Sites** pull-down list in the upper-right corner of the page.

Questions about adding, renewing, and moving licenses

Can I move a license from one computer to another?

Yes. You can uninstall the client software from one computer and install it on a new computer without affecting the total number of licenses you are using. The old computer is automatically subtracted from your total license count on the Total Protection Service accounting system, and the new one added, so that your license number remains constant. To do this:

1. Uninstall the software from the old computer.
2. From the SecurityCenter, click the **Computers** tab.
3. For Groups, select **All**, then select the old computer in the listing and click **Delete**.
4. Install the software on the new computer.

The new computer appears in your reports after it uploads its status to the SecurityCenter. This usually takes about 20 minutes.

My computer crashed and I had to reinstall the operating system and start over. Will this affect my license number?

No. The old computer is automatically subtracted from your total license count on the Total Protection Service accounting system, and the new one added, so that your license number remains constant.

1. From the SecurityCenter, click the **Computers** tab.
2. For Groups, select **All**, then select the old computer in the listing and click **Delete**.
3. Install the software on the reformatted computer.

The new computer appears in your reports after it uploads its status to the SecurityCenter. This usually takes about 20 minutes.

Using Virus and Spyware Protection

Virus and spyware protection checks for viruses, spyware, unwanted programs, and other potential threats by scanning files and programs each time they are accessed on client computers. It checks removable media, email messages and attachments, and network files. Users can manually request scans for any or all files, folders, and programs on their computers, and administrators can schedule scans to occur at regular intervals.

Virus and spyware protection functions as a single component within Total Protection Service, but includes policy options that let you configure some of the virus protection and spyware protection features separately. Virus and spyware protection includes optional features that let you or client computer users select the types of files and programs to scan and the types of threats to detect. You or the users can also specify files to exclude from virus scans and programs that should not be detected as spyware.

Contents

- How detections are handled
- Spyware protection mode and detections
- Types of scans
- Scanning on client computers
- Configuring scanning policy options
- Managing detections
- Reports for virus and spyware protection
- Best practices (virus and spyware protection)
- Frequently asked questions
- Error messages

How detections are handled

The type of threat and the policy settings determine how virus and spyware protection handles a detection.

Items with detections	How virus and spyware protection handles the detections
Files and programs	**Virus detections**: Virus and spyware protection attempts to clean the file. If it can be cleaned, the user is not interrupted with an alert. If it cannot be cleaned, an alert appears, and the detected file is deleted. A copy is placed in the quarantine folder. **Potentially unwanted program detections**: In Protect mode, detections are cleaned or deleted. In Prompt mode, users must select the response.
Items with detections	**How virus and spyware protection handles the detections**
	In all cases, a backup copy of the original item is saved in a quarantine folder, in a proprietary binary format. Data for all activity is uploaded to the SecurityCenter for use in reports. NOTE: Files are placed into the quarantine folder in a format that is no longer a threat to the client computer. It is not necessary to view or delete them, but you might occasionally want to do so. In these situations, you must view files on the client computer by using the Quarantine Viewer. Only users logged on as an administrator can access the Quarantine Viewer. After 30 days, these files are deleted.
Registry keys and cookies	Detections initially appear as **Detected**. Cleaning detected files also cleans their associated registry keys and cookies. Their status is then reported as **Cleaned**.

Spyware protection mode and detections

Spyware protection monitors programs that attempt to install or run on client computers. When it detects an unrecognized program, it either allows or blocks it. The response is based on the spyware protection mode selected in the policy assigned to the client computer.

In this mode...	Spyware protection does this...
Protect	Checks the list of allowed and blocked programs created by the administrator for computers using the policy. If the program is not on the list, spyware protection blocks the potentially unwanted program.
Prompt	Checks the list of approved and blocked programs created by the administrator for computers using the policy. Checks the list of programs the user has approved. If the program is not on either list, spyware protection displays a prompt with information about the detection and allows the user to select a response. This setting is the default.
Report	Checks the list of approved and blocked programs created by the administrator for computers using the policy. If the program is not on the list, it sends information about the potentially unwanted program to the SecurityCenter and takes no additional action.

For all modes, detections are reported to the SecurityCenter, where you can view information about them in reports.

NOTE: To prevent popup prompts from appearing on client computers when potentially unwanted programs are detected, and for highest security, we recommend using Protect mode.

How policy options are implemented in the three protection modes

Mode	Behavior of virus and spyware protection
Report	• Users are not prompted about detections. • Detections are reported to the SecurityCenter. • Administrator can select approved programs, which are not reported as detections. • Can be used as a "learn" mode to discover which programs to approve and block.
Prompt	• Users are prompted about detections. • Detections are reported to the SecurityCenter. • Administrator can select approved programs. These programs are not reported as detections, and users are not prompted for a response to them. • Users can approve additional programs in response to prompts. These are reported to the SecurityCenter.
Protect	• Users are not prompted about detections. • Users are notified about deleted or quarantined programs. • Detections are reported to the SecurityCenter. • Administrator can select approved programs, which are not reported as detections.

Use learn mode to discover programs

Report mode can be used as a "learn mode" to help you determine which programs to approve. In Report mode, spyware protection tracks but does not block potentially unwanted programs. You can review detected programs in the Unrecognized Programs report and approve those that are appropriate for your policy. When you no longer see unapproved programs you want to approve in the report, change the policy setting for spyware protection mode to Prompt or Protect.

Types of scans

Virus and spyware protection scans files automatically for viruses and spyware. At any time, users can perform manual scans of files, folders, or email, and administrators can set up scheduled scans. Policy options let you configure whether optional email and spyware scans occur.

- Automatic (on-access) scans
- Manual on-demand scans
- Scheduled on-demand scans
- Email scans
- Spyware scans

The behavior of the scanning features on client computers is defined in the policies configured in the SecurityCenter. Policy settings determine the types of files, programs, and other items detected; whether users can manage their detections; how frequently computers check for updates; and when scheduled scans occur.

On-access (automatic) scans

On-access scans are those that occur on client computers whenever users access files (for example, open a file or run a program).

Virus and spyware protection policy options let you configure these on-access scanning features:

- The types of files scanned and whether files on network drives are scanned.
- Whether email and attachments are scanned.
- Whether files in archives (compressed files, such as .zip files) are scanned.
- Whether files are scanned for spyware.
- The types of virus and spyware threats to detect.
- Whether unrecognized detections are sent to McAfee Avert Labs for investigation.
- Whether to enable on-access scanning (if it is disabled) whenever computers check for updates.
- Files and folders excluded from scans.
- Approved programs that should not be detected as threats.

The default settings for on-access scanning are:

- Scan all types of local files when opened, and again when closed (if they were modified). Do not scan files on network drives.
- Scan all email attachments when accessed and when saved to the hard drive, protecting the computer from email infections.
- Do not scan files in archives.
- Scan programs for spyware identifiers, to detect if a spyware program attempts to run or a program attempts to install spyware.
- Scan for all types of virus and spyware threats.
- Send unrecognized detections to McAfee Avert Labs.
- Enable on-access scanning when computers check for updates.

On-demand scans

On-demand scans are those that occur whenever administrators or users request them. Users can request on-demand scans to occur immediately, and administrators can schedule them to occur at regular intervals.

On-demand scans use many of the same policy options as on-access scans. In addition, virus and spyware protection policy options let you configure these on-demand scanning features:

- Whether files in archives (compressed files, such as .zip files) are scanned.
- A schedule for performing an on-demand scan at regular intervals.

The default settings for on-demand scans are:

- Scan all local files, including those in archives.
- Scan all critical registry keys.
- Scan all processes running in memory.
- Do not perform a scheduled scan.

In addition, during an on-demand scan of the My Computer folder, the drive where Windows is installed, or the Windows folder:

- Scan all cookies.
- Scan all registry keys.

NOTE: At the start of an on-demand scan, all previous detections of potentially unwanted programs are cleared from the Potentially Unwanted Program Viewer.

Scheduled scans

Schedule an on-demand scan to occur at a specific date and time, either once or on a recurring basis. For example, you might want to scan client computers at 11:00 P.M. each Saturday, when it is unlikely to interfere with other processes running on client computers.

Configure scheduled scans by selecting policy options for virus and spyware protection. Scheduled scans run on all computers using the policy.

Email scans

Email scans occur during on-access and on-demand scans.
A virus and spyware protection policy option lets you configure whether email is scanned before it reaches a users' Inbox.

The default settings for email scanning are:

- Scan all email attachments when accessed and when saved to the hard drive, protecting the computer from email infections.
- Scan email before placing it in a user's Inbox.

Spyware scans

Spyware scanning is a feature within virus and spyware protection that looks for and identifies spyware indicators. Spyware scanning occurs:

- Whenever programs are installed or run, as part of on-access scans.
- During on-demand scans.

Virus and spyware protection policy options let you configure these spyware scanning features:

- Whether files are scanned for spyware.
- The types of spyware threats to detect.
- Approved programs that should not be detected as threats.

The default spyware-related settings are:

- Look for spyware identifiers during on-access and on-demand scans, to detect if a spyware program attempts to run or a program attempts to install spyware.
- Scan for all types of spyware threats.

The response to detections depends on the spyware protection mode configured in the client computer's policy. Three responses are possible:

- Attempt to clean the program (Protect mode).
- Prompt the user for a response (Prompt mode).

This is the default setting.

- Report the detection and take no further action (Report mode).

Cookies and registry keys that indicate spyware are also detected. Deleting a potentially unwanted program deletes any associated cookies and registry keys.

All detections are listed in administrative reports available from the SecurityCenter. On client computers, users can view and manage detections by using the Potentially Unwanted Program Viewer.

NOTE: At the start of an on-demand scan, all previous detections of potentially unwanted programs are cleared from the Potentially Unwanted Program Viewer. For on-access scans, previous detections remain in the Potentially Unwanted Program Viewer.

Scanning on client computers

Use these tasks from a client computer to scan for threats on the computer and to temporarily disable the scanning feature for testing.

Tasks

►Scanning on demand from the console
►Scanning on demand from Windows Explorer
►Scanning email on client computers
►Viewing the progress of scheduled scans
►Enabling and disabling on-access scanning

Scanning on demand from the console

Use this task to perform a manual scan from the Total Protection Service console on a client computer.

Task

1 Click the Total Protection Service icon in the system tray, then select **Open Console**.

2 From the Action Menu, select **Scan Computer**.

3 Select the scan target.
- **Scan my entire computer** — Scan all drives, folders, and files.
- **Scan a specific drive or folder** — Type the full path and name of the scan target or browse to locate it.

4 Click **Start Scan**. Virus and spyware protection displays the progress of the scan.

5 If needed, click **Pause Scan** to temporarily interrupt the scan or **Cancel Scan** to end the scan. *(Optional)*

6 Click **View detailed report** to open a browser window and display the results of the scan.

Scanning on demand from Windows Explorer

Use this task to perform a manual scan from Microsoft Windows Explorer on a client computer.

Task

1 In Windows Explorer, right-click any drive or folder, then select **Scan Now**.

2 Close the Scan Completed panel or click **View detailed report** to display the Scan Statistics report.

Scanning email on client computers

Use this task to scan an email message manually on a client computer.

Task

1 In the Microsoft Outlook Inbox, highlight one or more messages in the right pane.

2 Under Tools, select **Scan for Threats**. The On-Demand Email Scan window displays any detections. If the window is empty, no threats were detected.

Viewing the progress of scheduled scans

Use this task to view a scheduled scan that is in progress on a client computer.

Before you begin

Enter your administrator credentials by using the Admin Login feature on the client computer.

Task

1 Click the Total Protection Service icon in the system tray, then select **Open Console**.

2 From the Action Menu, select **Product Details**.

3 In the Virus and Spyware Protection section, select **View Scheduled Scan**. Virus and spyware protection displays the progress of the scan.

NOTE: This option is available only when a scheduled scan is in progress.

4 If needed, click **Pause Scan** to temporarily interrupt the scan or **Cancel Scan** to end the scan. (*Optional*)

5 Click **View detailed report** to open a browser window and display the results of the scan.

Enabling and disabling on-access scanning

Use this task at the client computer to disable the on-access scanner temporarily, which is useful when working with product support to troubleshoot issues with scanning and cleaning files. Use the same task to re-enable on-access scanning.

NOTE: This task disables only on-access scanning. Buffer overflow protection continues to function. To disable buffer overflow protection, you must update the policy.

If you do not re-enable on-access scanning, it is enabled the next time the computer checks for updates (unless you have disabled the policy option).

Before you begin

Enter your administrator credentials by using the Admin Login feature on the client computer.

Task

1 Click the Total Protection Service icon in the system tray, then select **Open Console**.

2 From the Action Menu, select **Product Details**.

3 Under Virus and Spyware Protection, for On-access scanning, select the **Disable** option.

NOTE: If you disable on-access scanning, files are no longer checked for threats when they are accessed. We recommend that you re-enable this feature as soon as possible.

4 Under Virus and Spyware Protection, for On-access scanning, select the **Enable** option to re-enable the feature.

Configuring scanning policy options

Use these SecurityCenter tasks to configure policy options for virus and spyware scans performed on client computers.

Tasks

► Scheduling a scan
► Enabling optional types of virus scans
► Excluding files and folders from virus scans
► Selecting spyware scanning options
► Approving and unapproving programs in a policy

Scheduling a scan

Use this SecurityCenter task to schedule an on-demand scan.

Task

For option definitions, click **?** in the interface.

1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2 Click **Virus & Spyware Protection**, then click the **General Settings** tab.
3 Under Scheduled Scan Settings, select **On**.
4 Select a frequency, day, and time for the scan to run, then click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Enabling optional types of virus scans

Use this SecurityCenter task to specify optional scans and features for virus protection. If none of these features is selected, virus protection still detects viruses.

Task

For option definitions, click **?** in the interface.

1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2 Click **Virus & Spyware Protection**, then click the **Advanced Settings** tab.

3 Under Virus Protection Settings, select each scan you want to enable.

Select this option...	To do this...
Enable outbreak response	Check for an outbreak detection definition (DAT) file every hour.
Enable buffer overflow protection	Detect code starting to run from data in reserved memory and prevent that code from running. Virus and spyware protection protects against buffer overflow in more than 30 most commonly used Windows-based programs. McAfee updates this list as it adds buffer overflow protection for additional programs. CAUTION: Buffer overflow protection does not stop data from being written. Do not rely on the exploited application remaining stable after being compromised, even if buffer overflow protection stops the corrupted code from running.
Enable script scanning	Detect harmful code embedded in web pages that would cause unauthorized programs to run on client computers. NOTE: Script scanning is always enabled for on-access and on-demand scans.
Scan email (before delivering to the Outlook Inbox)	Look for threats in email before it is placed into the user's Inbox. (Email is always scanned when it is accessed.)
Scan all file types during on-access scans	Inspect all types of files, instead of only default types, when they are downloaded, opened, or run. (Default file types are defined in the DAT files.)
Scan within archives during on-access scans (e.g., .zip, .rar, .tat, .tgz)	Look for threats in compressed archive files when the files are accessed.
Scan within archives during on-demand scans (e.g., .zip, .rar, .tat, .tgz)	Look for threats in compressed archive files during manual or scheduled scans.
Enable Artemis hueristic network check for suspicious files	Send unrecognized threats to McAfee Avert Labs for investigation. (This occurs in the background with no user notification.)
Scan mapped network drives during on-access scans	Look for threats in files located on mapped network drives when the files are accessed.
Enable on-access scanning (if disabled) the next time client computers check for an update	If on-access scanning has been disabled on a client computer, re-enable it the next time that computer checks for updates.
Maximum percentage of CPU time allocated for on-demand and scheduled scans	Use up to the selected percentage of CPU resources when performing on-demand scans. When set to High, we recommend scheduling scans to occur during off-peak hours.

4 Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Excluding files and folders from virus scans

Use this SecurityCenter task to define and manage items that are not scanned for viruses. You can add files, folders, or file extensions to the list of exclusions or remove them from the list.

Task

For option definitions, click **?** in the interface.

1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click **Virus & Spyware Protection**, then click the **Excluded Files and Folders** tab.
3 Select the type of exclusion you want to create.
4 Specify the value (browse for a file or folder, or type a file extension).
5 Click **Add Exclusion**. The new exclusion appears in a list.
6 To remove an entry from the list of exclusions, click **Block**.
7 Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Selecting spyware scanning options

Use this task to configure policy options for spyware scanning features.

Task

For option definitions, click **?** in the interface.

1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2 Click **Virus & Spyware Protection**, then click the **General Settings** tab.
3 For Spyware Protection Status, select a protection mode to enable spyware protection, or select **Off** to disable spyware protection.
4 Click the **Advanced Settings** tab.
5 Under Spyware Protection Settings, select each type of program you want to detect.
6 Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Approving and unapproving programs in a policy

Use this SecurityCenter task to add approved programs to a policy or remove approved programs from a policy. Approved programs are not detected as potentially unwanted programs.

NOTE: You can also use the Unrecognized Programs report to view a complete listing of all programs detected on client computers and add them to policies.

Task

For option definitions, click **?** in the interface.

1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2 Click **Virus & Spyware Protection**, then click the **Approved Programs** tab.
3 Locate the program you want to approve in the listing of all programs detected on client computers, then select an option.

Select this...	To do this...
Approve	Approve the selected program.
Approve All	Approve all the programs listed.
Block	Block the selected program.
Block All	Block all the programs listed.

4 Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Managing detections

- Use these tasks to view and manage threats detected during virus and spyware scans.
- For an individual client computer, perform tasks at the computer (users and administrators).
- For multiple computers, groups, or an entire account, access administrative reports from the SecurityCenter.

Tasks

►Viewing scan results on client computers
►Managing potentially unwanted programs on client computers
►Viewing quarantined files on client computers
►Viewing user-approved programs and applications
►Viewing threats detected on the account
►Viewing unrecognized programs detected on the account

Viewing scan results on client computers

Users and administrators can use this task from a client computer to view the Scan Statistics report on a client computer after completing an on-demand scan.

NOTE: Client computers also send information about threats detected during scans to the SecurityCenter in encrypted XML files. Administrators can access three reports containing information about detected virus and spyware threats and potentially unwanted programs from the Reports page on the SecurityCenter.

Before you begin

Run an on-demand scan.

Task

- Select **View detailed report** in the Scan Completed panel. A browser window opens and displays the Scan Statistics report, which includes this information:
  - Date and time the scan was started.
  - Elapsed time for the scan.
  - Version of the scanning engine software and DAT file.
  - Date of the last update.
  - Completion status of the scan.
  - Location of the scanned items.
  - Status for scanned files, registry keys, and cookies.

Status	What it means...
Scanned	Number of items scanned.
Detected	The item is still a threat and still resides on the system. For files, they are most likely contained within a compressed archive (for example, a .ZIP archive) or on write-protected media. For registry keys and cookies, the file they are associated with has a status of Detected.
Cleaned	The item was cleaned of the threat. A backup copy of the original item was saved in a quarantine folder, in a proprietary binary format, where it can be accessed only with the Quarantine Viewer.
Deleted	The item could not be cleaned; it was deleted instead. A copy was saved in a quarantine folder, in a proprietary binary format, where it can be accessed only with the Quarantine Viewer.

Managing potentially unwanted programs on client computers

Users and administrators can use this task from a client computer to view and manage detections of potentially unwanted programs in the Potentially Unwanted Programs Viewer. It lists all items detected by spyware protection, which might include program files, registry keys, and cookies.

Task

1. Click the Total Protection Service icon in the system tray, then select **Open Console**.
2. In the Virus and Spyware Protection section, select **View Potentially Unwanted Programs**.
3. From the list of detections, select one or more items, then click an action.
   - **Clean** — Place an original copy of each selected item in a quarantine folder, in a proprietary binary format, then attempt to clean it. If it cannot be cleaned, delete the item.
   - **Approve** — Add selected items to the list of approved programs so they will not be detected as spyware.

   NOTE: Clicking **Approved** displays a list of all currently approved programs on your computer.
4. Check the status of each item.
   - **Action Required** — You have not performed any action on this item since it was detected.
   - **Approved** — The item was added to the list of user-approved programs and will no longer be detected as spyware.
   - **Cleaned** — The item was cleaned successfully and can be used safely. A backup copy of the original item was placed in a quarantine folder, in a proprietary binary format.
   - **Quarantined** — The item could not be cleaned. The original item was deleted and a copy was placed in a quarantine folder, in a proprietary binary format. If the item was a program, all associated cookies and registry keys were also deleted.

     NOTE: Items are placed into the quarantine folder in a format that is no longer a threat to your computer. These items are deleted after 30 days. Users with administrator rights can manage these items using the Quarantine Viewer.
5. Click **Back** to return to the console.

Viewing quarantined files on client computers

When virus and spyware protection detects a threat, it places a copy of the item containing the threat in a quarantine folder before cleaning or deleting the original item. The copy is stored in a proprietary binary format and cannot harm the computer. By default, items in the quarantine folder are deleted after 30 days.

Use this task from a client computer to view and manage quarantined items in the Quarantine Viewer. You must be logged on as an administrator to access this task.

Before you begin

Enter your administrator credentials by using the Admin Login feature on the client computer.

Task

1. Click the Total Protection Service icon in the system tray, then select **Open Console**.
2. From the Action Menu, select **Product Details**.
3. In the Virus and Spyware Protection section, select **View Quarantined Files**. The Quarantine Viewer lists all the items in the quarantine folder and their status.
4. Select one or more items, then click an action.
   - **Rescan** — Scan each selected item again. This option is useful when new detection definition (DAT) files include a method of cleaning a detection that could not be cleaned previously. In this case, rescanning the file cleans it and allows you to restore it for normal use.
   - **Restore** — Place each selected item back in its original location on your computer. The restored item will overwrite any other items with the same name in that location.

     NOTE: Virus and spyware protection detected this item because it considers the item to be a threat. Do not restore the item unless you are sure it is safe.
   - **Delete** — Remove each selected item from the quarantine folder, along with all associated registry keys and cookies. No copy will remain on your computer.
5. Check the status of each item:
   - **Cleaned** — The item was cleaned successfully and can be used safely. A backup copy of the original item was placed in a quarantine folder, in a proprietary binary format.
   - **Clean failed** — The item cannot be cleaned.
   - **Delete failed** — The item cannot be cleaned or deleted. If it is in use, close it and attempt the clean again. If it resides on read-only media, such as CD, no further action is required. Virus and spyware protection has prevented the original item from accessing your computer, but it cannot delete the item. Any items copied to your system have been cleaned.

     NOTE: If you are not sure why the item could not be cleaned, a risk might still exist.
   - **Quarantined** — You have not performed any action on this item since it was placed in the quarantine folder.
6. Select **Get more information on the threats detected** to open a browser window and visit the McAfee Avert Labs Threat Library.
7. Click **Back** to close the Quarantine Viewer and return to the console.

Viewing user-approved programs and applications

Use this task to see which applications users have approved to run on their computers. You can also add the applications to one or more policies so they will not be detected as unrecognized programs on computers using the policies.

Before you begin

Users can approve applications only when spyware protection mode or firewall protection mode is configured as Prompt mode.

Task

For option definitions, click **?** in the interface.

1 From the SecurityCenter, do any of the following:

- Click the **Computers** tab, then click a number in the User-Approved Applications column to view applications for the associated computer.
- Click the **Computers** tab, then click the name of a computer. In the Computer Details page, under Detections, click a number in the User-Approved Applications column to view applications.

2 To add the application to one or more policies, in the User-Approved Applications list, under Actions click **Allow**.

3 In the Add Approved Application page, select each policy where you want to add the application, then click **Save**.

Viewing threats detected on the account

Use this SecurityCenter task to view the Detections report, which lists these types of threats detected on all the client computers on your account:

- virus and malware threats
- potentially unwanted programs
- buffer overflow processes
- cookies

Task

For option definitions, click **?** in the interface.

1 Click the **Reports** tab, then click **Detections**.

2 In the Detections report, view detailed information about detections and the computers where detections occurred by using one of these methods.

When you want to...	Do this...
Display computers or detections	Click the triangle icon next to a name. • Under a computer name, show which detections were found. • Under a detection name, show the computers where it was found. Click a group name to display computers in that group.
View details about detections	If detections are listed for a computer, click a quantity to display details. • Click a quantity for Detected Objects to display a list of detected threats and their status. • From the Detections List, click the name of a detection to display detailed information from the McAfee Avert Labs Threat Library.
View details about a computer where a detection occurred	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.

Viewing unrecognized programs detected on the account

Use this SecurityCenter task to view the Unrecognized Programs report, which lists potentially unwanted programs detected on all the client computers on your account.

Task

For option definitions, click **?** in the interface.

1. Click the **Reports** tab, then click **Unrecognized Programs**.
2. In the Unrecognized Programs report, view detailed information about unrecognized programs and the computers where they were detected by using one of these methods.

When you want to...	Do this...
Display computers or detections	Click the triangle icon next to a name. • Under a computer name, show which programs were detected. • Under a program name, show the computers where it was detected. Click a group name to display computers in that group.
View details about detections	Click the name of a potentially unwanted program to display detailed information from the McAfee Avert Labs Threat Library.
View details about a computer where a detection occurred	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.
Approve a program	Click **Allow**, select one or more programs, select one or more policies where the programs will be approved, then click **Save**. The selected programs will no longer be detected as threats on computers using the selected policies.

Reports for virus and spyware protection

View information about virus and spyware detections in administrative reports available from the SecurityCenter. Reports provide details about the specific threats detected and the history of detections over the past year.

- Detections report — Lists the malware threats, potentially unwanted programs, buffer overflow processes, and cookies that virus and spyware protection detected on client computers.
- Unrecognized Programs report — Lists programs detected on client computers that are not recognized by spyware protection and firewall protection. Allows you to approve programs from within the report.
- Detection History report — Graphs detections on client computers over the past year.

Detections report

Use the Detections report to view and manage the types of potentially malicious code or unwanted programs that have been found on the network.

Select the information that appears in this report How to use this report

Select this option...	To do this...
Report period	Specify the period of time for which to display information. Select from the last week or one of the last 12 months.
Detection type	Show all threat detections or a particular type. • **Malware Infections** — Known threats that would infect the computer if they were not caught. • **Potentially Unwanted Programs** — Programs that you have not approved to run on client computers. • **Buffer Overflow Processes** — Unwanted code that attempted to run in reserved memory but was stopped. • **Cookies** — Data files containing personal information that are created by a web server and stored on your computer. Cookies allow web servers to recognize you and track your preferences when you visit Internet sites.
View	List the computers where detections occurred, the names of detections, or the groups containing computers where detections occurred.
Groups	Display all the computers on your account or only those in a single group.

How to use this report

When you want to...	Do this...
Display computers or detections	Click the triangle icon next to a name. • Under a computer name, show which detections were found. • Under a detection name, show the computers where it was found. Click a group name to display computers in that group.
View details about detections	If detections are listed for a computer, click a quantity to display details. • Click a quantity for Detected Objects to display a list of detected threats and their status. • From the Detections List, click the name of a detection to display detailed information from the McAfee Avert Labs Threat Library.
View details about a computer where a detection occurred	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.

Unrecognized Programs report

Use the Unrecognized Programs report to view a list of unapproved programs that spyware protection detected on the network. This list is cumulative — previously detected programs remain in the list, and new detections are added each time you access the report.

Select the information that appears in this report

Select this option...	To do this...
Report period	Specify the period of time for which to display information. Select from the last week or one of the last 12 months.
Detection type	Show all unrecognized programs, only programs blocked by firewall protection, only potentially unwanted programs, or only cookies.
View	List the computers where unrecognized programs were detected, the name of the programs, or the groups containing computers where unrecognized programs were detected.
Groups	Display all the computers on your account or only those in a single group.

How to use this report

When you want to...	Do this...
Display computers or detections	Click the triangle icon next to a name. • Under a computer name, show which programs were detected. • Under a program name, show the computers where it was detected. Click a group name to display computers in that group.
View details about detections	Click the name of a potentially unwanted program to display detailed information from the McAfee Avert Labs Threat Library.
View details about a computer where a detection occurred	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.
Approve a program	Click **Allow**, select one or more programs, select one or more policies where the programs will be approved, then click **Save**. The selected programs will no longer be detected as threats on computers using the selected policies.

Detection History report

Check the Detection History report for a graphical overview of the number of detections and the number of computers where detections occurred over the past year on your network. This information can help you determine how successfully your protection features have performed, and whether strategies you have implemented, such as user education or policy adjustments, have been effective.

Select the information that appears in this report

Select this option...	To do this...
Display by	Display information for the last year in monthly or quarterly increments.
Groups	Display all the computers on your account or only those in a single group.

Best practices (virus and spyware protection)

To develop an effective strategy for guarding against virus and spyware threats, we recommend that you proactively track the types of threats being detected on your network and where they are occurring.

1. Check your status emails or the SecurityCenter website for an overview of your account's status.
   - Ensure that computers in your account are up-to-date.
   - Ensure that protection is installed on all computers.
2. Check the Detections report regularly to see what is being detected.
3. Check the Unrecognized Programs report frequently to monitor the programs that users are approving on client computers. If you know some of the programs are safe and do not want them to be detected as potentially unwanted, add them to policies as approved programs.
4. To centralize management and more easily monitor the types of programs allowed on client computers, define client security settings in a policy.
5. If particular types of detections are occurring frequently or certain computers appear vulnerable, update the policy to resolve these issues.
   - Schedule scans or add exclusions.
   - Enable advanced scanning options.
   - Ensure that spyware protection is enabled.
   - For maximum protection, set your spyware protection mode to Protect to automatically clean potentially unwanted programs.

     NOTE: Protect mode is not the default setting. For maximum protection, create a policy that includes Protect mode.
   - Enable all advanced spyware options.
6. Use "learn" mode to identify which programs to add to the Approved Programs list. This ensures that no required programs are deleted before you have the opportunity to authorize their use. Then change your spyware protection mode to Protect.
7. View the Detection History report periodically to discover trends specific to your network, and verify your strategy's success in reducing detections.

Frequently asked questions

This section includes questions asked by administrators that are related to using policy options for virus and spyware protection.

How can I prevent popup prompts from appearing when unrecognized programs are detected?

Virus and spyware protection prompts users for a response to a potentially unwanted program detection when set to Prompt mode. To prevent popups, select Protect or Report mode. For highest protection, select Protect to automatically delete unrecognized programs.

Why would I want to specify excluded files and folders or approved programs?

Specifying excluded files and folders from scanning can be useful if you know a particular type of file is not vulnerable to attack, or a particular folder is safe. If you use a program to

conduct your business, adding it to a list of approved programs keeps it from being detected as unrecognized and deleted. If you are unsure, it is best not to specify exclusions.

Can I add approved programs to the McAfee Default policy?

No. However, you can create a new policy and add them. When you click **Add Policy** on the Policies page of the SecurityCenter, the new policy is prepopulated with the McAfee Default policy settings. Specify a name for the new policy, save it, and then add approved programs as needed. You can also designate the new policy as your default policy.

Error messages

This section includes error messages that are related to using the features of virus and spyware protection.

File does not exist.

This error verifies that the computer is protected from threats. When you clicked to open an infected file from Windows Explorer, the on-access scanner immediately detected and deleted the file, so that Windows could not open it.

On-access scan is currently disabled.

This error can be caused by several problems, but the most common solutions are:

- Check your connection to the network server or Internet.
- This feature has been disabled. From the client computer, log on as an administrator (using the Admin Login feature), then enable it from the Total Protection Service console on the client computer.

  NOTE: To prevent this problem, force the computer to re-enable on-access scanning automatically whenever it checks for updates by enabling the associated virus and spyware policy option.

Using Firewall Protection

Firewall protection checks for suspicious activity in communications sent between client computers and network resources or the Internet. As the administrator, you can define what constitutes suspicious activity and how firewall protection responds to:

- IP addresses and communication ports that attempt to communicate with your computer. You can specify whether to allow or block communications from other IP addresses on your network or outside your network, or you can identify specific IP addresses and ports to allow or block.
- Applications that attempt to access the Internet. You can use McAfee's recommendations for safe Internet applications, or you can identify specific applications to allow or block. You can also select firewall protection's response to detections of unrecognized applications.

Firewall protection has two primary modes: users configure firewall settings and an administrator configures firewall settings. The McAfee default policy is configured to let client computer users decide which communications and applications firewall protection allows. The administrator setting puts all or partial control with the administrator.

NOTE: To ensure the highest level of protection for your network, McAfee recommends that an administrator configure the firewall protection settings in one or more policies, which are then assigned to client computers. When an administrator sets firewall protection, it is important that the applications and communications that are important to your users are allowed before deploying the policy. This ensures that no important communications are blocked.

Contents

- Connection type and detections of incoming communications
- Firewall protection mode and detections of unknown applications
- The role of IP addresses
- The role of system service ports
- Firewall configuration
- Configuring policy options
- Configuring custom connections
- Installing and enabling firewall protection at the policy level
- Managing detections
- Reports for firewall protection
- Best practices (firewall protection)
- Frequently asked questions

Connection type and detections of incoming communications

Firewall protection monitors communications coming into the network (known as inbound events) to determine whether they meet criteria specified for safe communications. If an event does not meet the criteria, it is blocked from reaching computers on the network.

Specify criteria by selecting the type of connection client computers are using. A policy option setting determines whether the administrator or the user selects the connection type.

Types of connections

The connection type defines the environment where client computers are used, It determines what firewall protection considers to be suspicious activity and, therefore, which IP addresses and ports are allowed to communicate with the network computers.

Select from three connection environments.

Select this...	When the computer...	Then firewall protection...
Untrusted network	Is connected directly to the Internet. For example: through a dial-up connection, a DSL line, or a cable modem; through any type of connection in a coffee shop, hotel, or airport.	Blocks communications with all other computers, including those on the same subnet. This is the default setting.
Trusted network	Is connected indirectly to a network that is separated from the Internet by a hardware router or firewall. For example: in a home or office network.	Allows communications with other computers on the same subnet, but blocks all other network communications.
Custom	Should communicate only through specific ports or with a specific range of IP addresses, or the computer is a server providing system services.	Allows communications with the ports and IP addresses you specify, blocks all other communications. When you select this option, an **Edit** button becomes available that enables you to configure options.

Additional information about connection types

It is important to update the connection type whenever the working environment changes. For example, mobile users who connect to both secured (trusted) and unsecured (untrusted) networks must be able to change their setting accordingly.

A policy option specifies whether firewall protection tracks blocked events for reporting purposes. When the option is enabled, you can see a listing of all blocked events in the report entitled Inbound Events Blocked by Firewall.

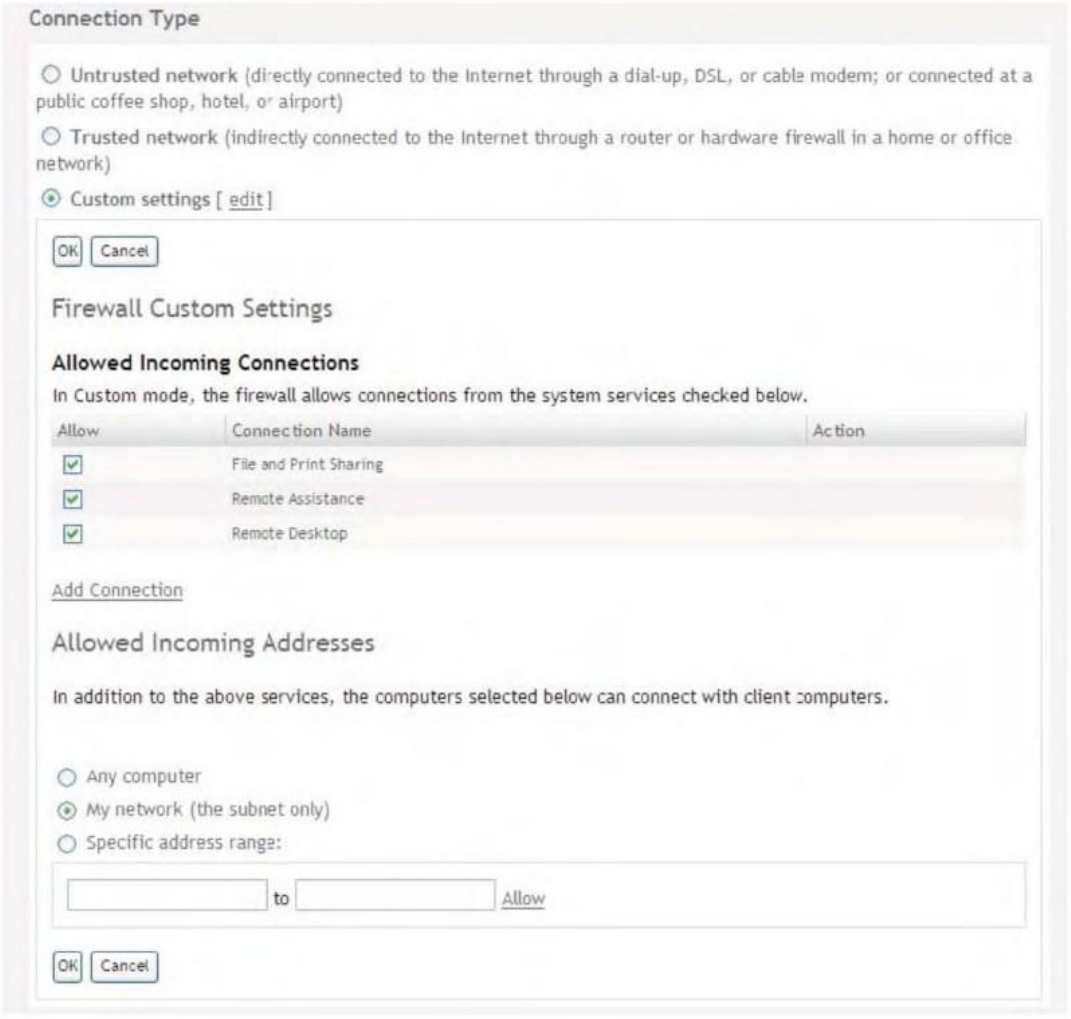
The connection type does not affect the way that firewall protection handles detections of Internet applications running on client computers.

Custom connections

Trusted and untrusted connection types let you specify whether to allow or block communications originating within a network. Configure a custom connection type when you want to be more specific about where communications originate. When you set up a custom connection, you can designate:

- Open and blocked ports, through which a computer can and cannot receive communications. This is required to set up a computer as a server that provides system services. The server will accept communications through any open port from any computer. Conversely, it will not accept communications through any blocked port.
- IP addresses from which a computer can receive communications. This allows you to limit communications to specific IP addresses.

Configure settings for custom connections on the General tab of the Firewall Protection policy page.



Once configured, custom connection settings are saved until you reconfigure them. If you temporarily select a Trusted network or Untrusted network connection type, the custom settings will still be there the next time you want to configure a custom connection.

NOTE: Custom settings configured on the SecurityCenter are ignored on client computers if firewall protection mode is set to Prompt. In Prompt mode, settings configured by users override administrator settings.

Firewall protection mode and detections of unknown applications

Firewall protection monitors communications with Internet applications, which connect to the Internet and communicate with client computers. When it detects an Internet application running on a computer, it either allows the application to connect to the Internet or blocks the connection. The response is based on the firewall protection mode selected in the policy assigned to the client computer.

In this mode...	Firewall protection does this...
Protect	Blocks the suspicious activity.
Prompt	Displays a dialog box with information about the detection, and allows the user to select a response. This setting is the default.
Report	Sends information about suspicious activity to the SecurityCenter and takes no additional action.

For all modes, detections are reported to the SecurityCenter, where you can view information about them in reports.

NOTE: To prevent popup prompts from appearing on client computers when applications are detected, and for highest security, we recommend using Protect mode.

How policy options are implemented in the three protection modes

Use the following table to determine how policy options are implemented in the different protection modes.

Mode	Behavior of firewall protection
Report	• Users are not prompted about detections. • Detections are reported to the SecurityCenter. • Administrator can select allowed applications, which are not reported as detections. • Can be used as a "learn" mode to discover which applications to allow and block.
Prompt	• Users are prompted about detections. • Detections are reported to the SecurityCenter. • Administrator can select allowed applications. These applications are not reported as detections, and users are not prompted for a response to them. • Users can approve additional applications in response to prompts. These are reported to the SecurityCenter.
Protect	• Users are not prompted about detections. • Users are notified about blocked applications. • Detections are reported to the SecurityCenter. • Administrator can select allowed applications, which are not reported as detections.

NOTE: If the policy is changed from Prompt mode to Protect mode or Report mode, firewall protection saves user settings for allowed applications. If the policy is then changed back to Prompt mode, these settings are reinstated.

Use learn mode to discover Internet applications

Report mode can be used as a "learn mode" to help you determine which applications to allow. In Report mode, firewall protection tracks but does not block unrecognized Internet applications. You can review detected applications in the Unrecognized Programs report and approve those that are appropriate for your policy. When you no longer see applications you want to allow in the report, change the policy setting to Prompt or Protect mode.

The role of IP addresses

An IP address is used to identify any device that originates or receives a request or a message over networks and the Internet (which comprises a very large group of networks). Each IP address uses a unique set of hexadecimal characters to identify a network, a subnetwork (if applicable), and a device within the network.

An IP address enables:

- The request or message to be delivered to the correct destination.
- The receiving device to know where the request or message originated and where to send a response if one is required.

Total Protection Service allows you to configure a custom connection to accept only communications that originate from designated IP addresses. You can specify IP addresses that conform to either of these standards:

- IPv4 (Internet Protocol Version 4) — The most common Internet addressing scheme. Supports 32-bit IP addresses consisting of four groups of four numbers between 0 and 255.
- IPv6 (Internet Protocol Version 6) — Supports 128-bit IP addresses consisting of eight groups of four hexadecimal characters.

The role of system service ports

System services communicate through ports, which are logical network connections. Common Windows system services are typically associated with particular service ports, and your computer's operating system or other system applications might attempt to open them. Because these ports represent a potential source of intrusions into a client computer, you must open them before the computer can communicate through them.

Certain applications, including web servers and file-sharing server programs, must accept unsolicited connections from other computers through designated system service ports. When configuring a custom connection, you can:

- Allow applications to act as servers on the local network or the Internet.
- Add or edit a port for a system service.
- Disable or remove a port for a system service.

NOTE: Select a port for system services only if you are certain it must be open. You will rarely need to open a port. We recommend that you disable unused system services.

Examples of system services that typically require ports to be opened are:

- **Email server** — You do not need to open a mail server port to receive email. You need to open a port only if the computer running firewall protection acts as an email server.
- **Web server** — You do not need to open a web server port to run a web browser. You need to open a port only if the computer running firewall protection acts as a web server.

NOTE: An opened service port that does not have an application running on it poses no security threat. However, we recommend that you close unused ports.

Standard assignments for system service ports

These commonly used standard service ports are listed by default, where you can open or close them:

- File and Print Sharing
- Remote Desktop
- Remote Assistance

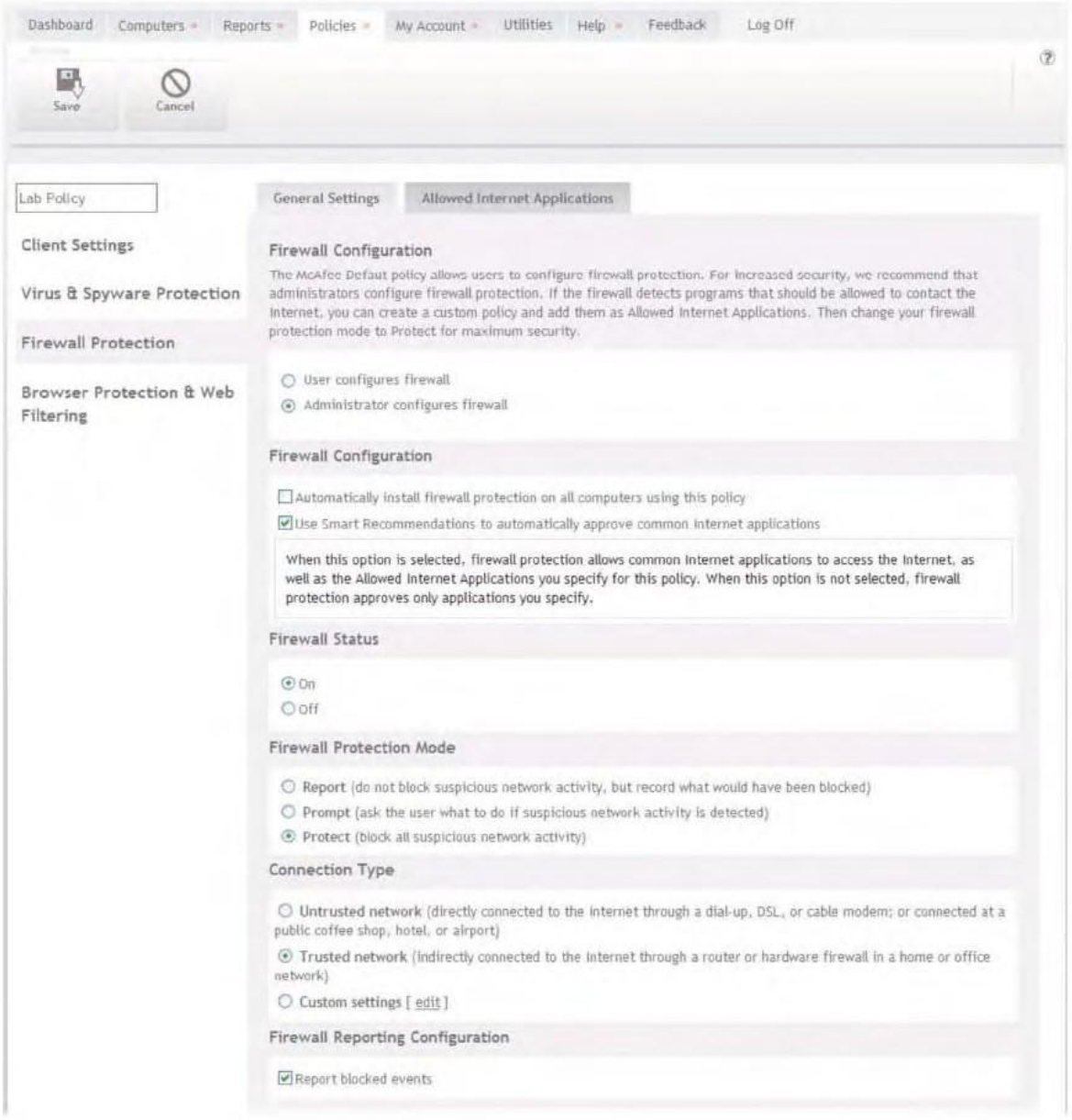
You can add other service ports as needed. Standard service ports for typical system services are:

System Service	Port(s)
File Transfer Protocol (FTP)	20-21
Mail Server (IMAP)	143
Mail Server (POP3)	110
Mail Server (SMTP)	25
Microsoft Directory Server (MSFT DS)	445
Microsoft SQL Server (MSFT SQL)	1433
Network Time Protocol Port	123
Remote Assistance / Terminal Server (RDP)	3389 (same as Remote Assistance and Remote Desktop)
Remote Procedure Calls (RPC)	135
Secure Web Server (HTTPS)	443
Universal Plug and Play (UPNP)	5000
Web Server (HTTP)	80
Windows File Sharing (NETBIOS)	137-139 (same as File and Print Sharing)

Firewall configuration

Protecting computers from suspicious activity with a firewall involves monitoring network activity to identify applications, IP addresses, and ports, and blocking those that could cause harm. There are two methods of establishing firewall protection:

- The administrator configures firewall settings in a Total Protection Service policy.
- Each client computer user configures firewall settings for their computer.



For the highest level of security, McAfee recommends that administrators configure firewall settings. If you allow users to configure the settings, it is important to educate them about threats and strategies for avoiding risk.

Configuring firewall features enables you, the administrator, to control which applications and communications are allowed on your network. It provides the means for you to ensure the highest level of security.

You can also allow users to configure their own firewall protection settings. In this case, no other firewall policy options are available for you to select. This is the default setting.

Interaction between user and administrator policy settings

Firewall protection handles the settings that you and users configure in a special way. This enables settings to be controlled by either you or the users at different times.

Settings that users select are never discarded, but whether they are used depends on the policy settings assigned to their computers. These also determine whether options for configuring firewall protection settings are displayed in the client console.

If you configure...	User settings are...	Configuration options display in the console?
No policy settings	Active	Yes
Firewall protection mode as either: • Protect • Report	Inactive	No
Firewall protection mode as Prompt	Merged with administrator settings. When they differ, user settings take precedence. For example, if a user approves a program, it is allowed even if the administrator has not approved it.	Yes

Configuring policy options

Use these tasks to select policy options for firewall behavior on client computers.

Tasks

►Selecting general firewall settings
►Configuring options for Internet applications
►Tracking blocked communications

Selecting general firewall settings

Use this task to configure these settings for firewall protection:

- Who configures the firewall
- Connection type

NOTE: To ensure the highest level of security, we recommend that administrators configure firewall settings. If you allow users to configure the settings, it is important to educate them about threats and strategies for avoiding risk.

Task

For option definitions, click **?** in the interface.

1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Select **Firewall Protection**, then click the **General Settings** tab.

3 Under Firewall Configuration, select **Administrator configures firewall** or **User configures firewall**. If you select the administrator option, additional policy options are displayed for you to configure.

4 Under Connection Type, select an option.

5 If you selected Custom, click **Edit** to configure related options. These are described in another section of this document.

6 Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Configuring options for Internet applications

Use this SecurityCenter task to configure the way firewall protection responds to detections of Internet applications by configuring these options:

- Whether firewall protection checks the list of Internet applications that McAfee has determined to be safe at the www.hackerwatch.org website.
- Whether firewall protection blocks an unrecognized application, prompts users for a response, or simply reports it to the SecurityCenter.
- Specific applications to allow or block

Before you begin

On the Firewall Protection policy page, you must select **Administrator configures firewall** before you can perform this task.

Task

For option definitions, click **?** in the interface.

1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Select **Firewall Protection**, then click the **General Settings** tab.

3 Under Firewall Configuration, select or deselect the **Use Smart Recommendations to automatically approve common Internet applications** option.

4 Under Firewall Protection Mode, select an option.

5 Click the **Allowed Internet Applications** tab. This tab lists all the Internet applications detected on the computers in your account.

6 Select options as needed.

Select this...	To do this...
Allow	Allow the application.
Allow All	Allow all the applications listed.
Block	Block the application.
Block All	Block all the applications listed.

7 Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Tracking blocked communications

Use this SecurityCenter task to track communication attempts (known as *events*) between client computers and network resources that firewall protection blocks. View information about these events in the report entitled Inbound Events Blocked by the Firewall.

Before you begin

On the Firewall Protection policy page, you must select **Administrator configures firewall** before you can perform this task.

Task

For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Firewall Protection**, then click the **General Settings** tab.
3. Under Firewall Reporting Configuration, select **Report blocked events**.
4. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Configuring custom connections

Use these tasks to configure system service ports and IP addresses for custom connections.

Tasks

►Configuring system services and port assignments
►Configuring IP addresses

Configuring system services and port assignments

Use this task to configure system service port assignments for a custom connection. This task allows you to add, remove, or modify a service by specifying its name and the ports through which it communicates with client computers using the policy.

Opening a system service port on a client computer allows it to act as a server on the local network or Internet. Closing a port blocks all communications through the ports with client computers using the policy.

Before you begin

On the Firewall Protection policy page, you must select **Administrator configures firewall** before you can perform this task. You must also select a Firewall Protection Mode of Protect or Report.

Task

For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Firewall Protection**, then click the **General Settings** tab.
3. Under Connection Type, select **Custom settings**, then click **edit**.

4 On the Firewall Custom Settings panel, under Allowed Incoming Connections, configure a service by using one of these methods.

To do this...	Perform these steps...
Allow an existing service by opening its ports	**1** Select the checkbox for a service listed in the table. **2** Click **OK**. Computers using this policy will accept communications through the ports assigned to the service.
Add a new service and open its ports	**1** Click **Add Connection**. **2** In the Add or Edit Incoming Connection panel, type a name for the service, type the ports through which the service will communicate with computers using this policy, then click **OK**.
Modify an existing service	**1** For a service listed in the table, click **edit**. **2** In the Add or Edit Incoming Connection panel, modify the name for the service and/or the ports through which the service will communicate with computers using this policy, then click **OK**.
Block an existing service and close its ports	**1** For a service listed in the table, click **Block**. **2** Click **OK**. The service is removed from the list, and computers using this policy will not accept communications through the ports assigned to the blocked service.

5 Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Configuring IP addresses

Use this task to add or remove a range of IP addresses in a custom connection. Client computers using this policy will accept communications originating only from the IP addresses you add.

NOTE: Specify IP addresses and system service ports through which to communicate by using separate tasks.

Before you begin

On the Firewall Protection policy page, you must select **Administrator configures firewall** before you can perform this task. You must also select a Firewall Protection Mode of Protect or Report.

Task

For option definitions, click **?** in the interface.

1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Select **Firewall Protection**, then click the **General Settings** tab.

3 Under Connection Type, select **Custom settings**, then click **edit**.

4 On the Firewall Custom Settings panel, under Allowed Incoming Addresses, configure a range of IP addresses for computers using this policy by using one of these methods.

To do this...	Perform these steps...
Accept communications from any IP address	**1** Select **Any computer**. **2** Click **OK**.
Accept communications from IP addresses on the subnet where the computers are located	**1** Select **My network (the subnet only)**. **2** Click **OK**.
Accept communications from the specified addresses	**1** Select **Specific address range**. **2** Type a beginning and ending IP address range in either IPv4 or IPv6 format. **3** Click **Approve**. The IP address range is displayed in a the list of allowed addresses. Computers using this policy will accept communications originating from all IP addresses in this list. **4** Click **OK**.
Block an existing range of IP addresses	**1** For the IP address range, click **Block**. The IP address range is removed from the list of allowed addresses. **2** Click **OK**. Computers using this policy will not accept communications originating from the IP addresses you removed from the list.

NOTE: When using a computer in multiple locations, you might want to specify more than one range of IP addresses. For example, you might want one IP address range for office use and another for home use. To specify multiple address ranges, repeat step 4, enter another address range, then click **Add** again.

5 Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Installing and enabling firewall protection at the policy level

Use these tasks to install or enable firewall protection automatically for all computers using the policy.

Tasks

► Installing firewall protection during policy updates
► Enabling and disabling firewall protection

Installing firewall protection during policy updates

Use this task to install firewall protection automatically whenever client computers check for an updated policy. You might want to use this feature for adding firewall protection on computers where the Total Protection Service client software is already installed. By default, this option is disabled.

NOTE: Enabling this feature can result in unattended installations on computers where no one is available to authorize communications that are consequently blocked by firewall protection. If this feature is used to install firewall protection on a server, it is important to configure essential system services first, to prevent disruptions.

Before you begin

On the Firewall Protection policy page, you must select **Administrator configures firewall** before you can perform this task.

Task

For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Firewall Protection**, then click the **General Settings** tab.
3. Under Firewall Configuration, select **Automatically install firewall protection on all computers using this policy**.
4. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Enabling and disabling firewall protection

Use this task to enable or disable firewall protection on all client computers using the policy.

Before you begin

On the Firewall Protection policy page, you must select **Administrator configures firewall** before you can perform this task.

Task

For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Firewall Protection**, then click the **General Settings** tab.
3. Under Firewall Status, select **On** or **Off**.
4. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Managing detections

Use these tasks to view and manage suspicious activity and unrecognized applications detected by firewall protection.

Tasks

►Viewing unrecognized programs detected on the account
►Viewing user-approved programs and applications
►Viewing blocked communications

Viewing unrecognized programs detected on the account

Use this SecurityCenter task to view the Unrecognized Programs report, which lists potentially unwanted programs detected on all the client computers on your account.

Task

For option definitions, click **?** in the interface.

1 Click the **Reports** tab, then click **Unrecognized Programs**.

2 In the Unrecognized Programs report, view detailed information about unrecognized programs and the computers where they were detected by using one of these methods.

When you want to...	Do this...
Display computers or detections	Click the triangle icon next to a name. • Under a computer name, show which programs were detected. • Under a program name, show the computers where it was detected. Click a group name to display computers in that group.
View details about detections	Click the name of a potentially unwanted program to display detailed information from the McAfee Avert Labs Threat Library.
View details about a computer where a detection occurred	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.
Approve a program	Click **Allow**, select one or more programs, select one or more policies where the programs will be approved, then click **Save**. The selected programs will no longer be detected as threats on computers using the selected policies.

Viewing user-approved programs and applications

Use this task to see which applications users have approved to run on their computers. You can also add the applications to one or more policies so they will not be detected as unrecognized programs on computers using the policies.

Before you begin

Users can approve applications only when spyware protection mode or firewall protection mode is configured as Prompt mode.

Task

For option definitions, click **?** in the interface.

1 From the SecurityCenter, do any of the following:

- Click the **Computers** tab, then click a number in the User-Approved Applications column to view applications for the associated computer.
- Click the **Computers** tab, then click the name of a computer. In the Computer Details page, under Detections, click a number in the User-Approved Applications column to view applications.

2 To add the application to one or more policies, in the User-Approved Applications list, under Actions click **Allow**.

3 In the Add Approved Application page, select each policy where you want to add the application, then click **Save**.

Viewing blocked communications

Use this task to view a list of communications that firewall protection prevented from reaching client computers. For the purposes of this report, each attempt to communicate is called an event.

Before you begin

To view this report, the **Report blocked events** option must be enabled on the Firewall Protection policy tab. When this option is enabled, blocked events are logged for all computers using the policy.

Task

For option definitions, click **?** in the interface.

1 Click the **Reports** tab, then click **Inbound Events Blocked by Firewall**.

2 In the report, view detailed information about detections and the computers where detections occurred by using one of these methods.

When you want to...	Do this...
Display computers or detections	Click the triangle icon next to a name. • Under a computer name, show which detections were found. • Under a detection name, show the computers where it was found. Click a group name to display computers in that group.
View details about events	Click a quantity under **Events** to display the Inbound Event List, which shows the name of the event, the number of occurrences, and the date on which it was detected.
View details about a computer	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.

Reports for firewall protection

You can view information about firewall detections in administrative reports available from the SecurityCenter. Reports provide details about the specific threats detected over the past year.

- Unrecognized Programs — Lists programs detected on client computers that are not recognized by virus and spyware protection and firewall protection. Allows you to approve Internet applications from within the report.
- Inbound Events Blocked by Firewall — Lists the incoming communication attempts that firewall protection prevented client computers from receiving, where they originated, and to which computer they were sent.

Unrecognized Programs report

Use the Unrecognized Programs report to view a list of unapproved Internet applications that firewall protection detected on your network. This list is cumulative — previously detected programs remain in the list, and new detections are added each time you access the report.

Select the information that appears in this report

Select this option...	To do this...
Report period	Specify the period of time for which to display information. Select from the last week or one of the last 12 months.
Detection type	Show all unrecognized programs, only programs blocked by firewall protection, only potentially unwanted programs, or only cookies.
View	List the computers where unrecognized programs were detected, the name of the programs, or the groups containing computers where unrecognized programs were detected.
Groups	Display all the computers on your account or only the computers in a single group.

How to use this report

When you want to...	Do this...
Display computers or detections	Click the triangle icon next to a name. • Under a computer name, show which applications were detected. • Under an application name, show the computers where it was detected. Click a group name to display computers in that group.
View details about a computer where a detection occurred	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.
Allow an Internet application	Click **Allow**, select one or more applications, select one or more policies where this application will be approved, then click **Save**. The selected applications will no longer be detected as a threat by firewall protection on computers using the selected policies.

Inbound Events Blocked by Firewall report

Use the Inbound Events Blocked by Firewall report to view a list of communications that firewall protection prevented from reaching client computers. For the purposes of this report, each attempt to communicate is called an *event*.

NOTE: To view this report, the **Report blocked events** option must be enabled on the Firewall Protection policy tab. When this option is enabled, blocked events are logged for all computers using the policy.

Select the information that appears in this report

Select this option...	To do this...
Report period	Specify the period of time for which to display information. Select from the last week or one of the last 12 months.
View	List the computers where inbound events were blocked, the computers where inbound events originated, or groups containing computers where inbound events were blocked.
Groups	Display all the computers on your account or only the computers in a single group.

How to use this report

When you want to...	Do this...
Display computers or detections	Click the triangle icon next to a name. • Under a computer name, show which detections were found. • Under a detection name, show the computers where it was found. Click a group name to display computers in that group.
View details about events	Click a quantity under **Events** to display the Inbound Event List, which shows the name of the event, the number of occurrences, and the date on which it was detected.
View details about a computer	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.

Best practices (firewall protection)

To effectively manage your strategy for guarding against suspicious activity, we recommend that you proactively track the types of threats being detected and where they are occurring.

1. Check your status emails or the SecurityCenter website for an overview of your account's status. Ensure that protection is installed on all computers.
2. To centralize management and more easily monitor the types of applications and communications allowed on client computers, configure client firewall protection settings in a policy.
3. Use McAfee's recommendations for commonly used, safe Internet applications. When this option is enabled, applications rated safe on McAfee's www.hackerwatch.org site are approved automatically, minimizing the need for you or users to approve applications manually.
4. Check the Unrecognized Programs report frequently to monitor the Internet applications that users are allowing on client computers. If you know some of the applications are safe and do not want them to be detected as threats, add them to policies.
5. If you want to monitor the inbound communications that firewall protection has blocked, select the **Report blocked events** policy option, then check the Inbound Events Blocked by Firewall report regularly.

6 Use "learn" mode to identify which Internet applications to allow. This ensures that no applications required for your business are blocked before you have the opportunity to authorize their use. Then change the protection mode to Protect.

7 If particular types of suspicious activity are occurring frequently or certain computers appear vulnerable, update the policy to resolve these issues.
   - Ensure that firewall protection is enabled.
   - Carefully specify the environment where client computers are used. For users with mobile computers, ensure that they know how to select the correct connection type each time their environment changes and that their policy allows them to do so.
   - Before installing firewall protection on a server, ensure that the server's system services and Internet applications are configured correctly. If there is a possibility that firewall protection might be installed when no user is present to monitor the installation, disable the policy setting for **Automatically install the desktop firewall on all computers using this policy**.
   - When running firewall protection on a server, ensure that system service ports are configured correctly to prevent disruption of system services. Ensure that no unnecessary ports are open.
   - For maximum protection, set firewall protection to Protect mode to automatically block suspicious activity.

8 If your account includes computers that are operated in multiple environments, such as in the office and in unsecured public networks, update the policy appropriately.
   - Configure policy options that allow users to select their connection type to match their environment. Be sure they know when and how to select the appropriate connection type.
   - If you configure custom connections that include IP addresses, specify ranges of IP addresses appropriate for all their working environments.

Frequently asked questions

This section includes questions asked by administrators and client computer users that are related to using these features of firewall protection.

- Policies
- General issues

Questions about policies

How can I prevent popup prompts from appearing when unrecognized programs are detected?

Firewall protection prompts users for a response to an Internet application detection when set to Prompt mode. To prevent popups, select Protect or Report mode. For highest protection, select Protect to automatically delete unrecognized Internet applications.

Can I add allowed Internet applications to the McAfee Default policy?

No. However, you can create a new policy and add them. When you click **Add Policy** on the Policies page of the SecurityCenter, the new policy is prepopulated with the McAfee Default policy settings. Specify a name for the new policy, save it, and then add allowed Internet applications as needed.

Questions about general firewall protection

Is it okay to run the Windows firewall and Total Protection Service firewall protection at the same time?

We recommend that you disable the Windows firewall when firewall protection is running. (It is disabled automatically when firewall protection is installed.)

If both firewalls are enabled, firewall protection lists only a subset of the blocked IP addresses in its report, Inbound Events Blocked by the Firewall. The Windows firewall blocks some of these addresses; however, it does not report them because event logging is disabled in the Windows firewall by default. If both firewalls are enabled, you must enable Windows firewall logging to be able to view a list of all blocked IP addresses. The default Windows firewall log is C:\Windows\pfirewall.log. In addition, there will be some duplication of status and alert messaging.

I blocked Internet Explorer on a client computer, and then temporarily disabled firewall protection. When I re-enabled firewall protection, why was Internet Explorer no longer blocked?

Firewall protection uses Internet Explorer to update product components. Whenever you enable firewall protection, Internet Explorer is given full access to check for updates.

Using Browser Protection and Web Filtering

Browser protection, based on McAfee SiteAdvisor,® displays information to safeguard client computer users against web-based threats:

- A safety rating for each website.
- A safety report for each website that includes a detailed description of test results and feedback submitted by users and site owners.

The web filtering module, available with some versions of Total Protection Service, provides features for regulating access to websites. Policy options allow administrators to control access to sites based on their safety rating, the type of content they contain, and their URL or domain name.

Contents

▶ Browser protection features
▶ How safety ratings are compiled
▶ Safety icons and balloons protect during searches
▶ SiteAdvisor menu protects while browsing
▶ Safety reports provide details
▶ Information that browser protection sends to McAfee
▶ Installing browser protection during policy updates
▶ Web filtering features
▶ Enabling and disabling browser protection via policy
▶ Enabling and disabling protection at the client computer
▶ Block and warn sites by content
▶ Authorize and prohibit sites by URL or domain
▶ Customizing messages for users
▶ Viewing browsing activity
▶ Web Filtering report
▶ Best practices (browser protection)
▶ Frequently asked questions

Browser protection features

As browser protection runs on client computers, it notifies users about threats they might encounter when searching or browsing websites by displaying the following:

Safety rating for each site and site resource

- When searching, safety ratings of green, yellow, red, and gray icons appear next to each site listed on a search results page.
- When browsing, the SiteAdvisor menu button appears in the browser window in the color that matches the safety rating for the current site.

Safety report for each site

- The report includes a detailed description of test results and feedback submitted by users and site owners.
- Users access safety reports to learn more about how the safety rating for a site was calculated.

Browser protection supports these browsers:

- Microsoft Internet Explorer browser (version 6.0 with Service Pack 1 or later)
- Mozilla Firefox browser (version 2.0 or later)

NOTE: The only difference in functionality between the browsers is that Firefox does not allow users to hide the SiteAdvisor menu button with the **View | Toolbars** command or check file downloads.

Web filtering features

Some versions of Total Protection Service include the web filtering module, which provides features that enable you to monitor and regulate browser activity on network computers.

- Control user access to websites and file downloads, based on their safety rating or type of content.
- Create a list of authorized and prohibited sites, based on their URL or domain.
- Block user access to phishing pages.
- Customize the message that browser protection displays on computers that attempt to access a blocked website.

Web filtering policy options also allow you to disable browser protection at the policy level or from an individual client computer.

Web filtering features are described in more detail later in this section.

How safety ratings are compiled

A McAfee team derives safety ratings by testing a variety of criteria for each site and evaluating the results to detect common threats.

Automated tests compile safety ratings for a website by:

- Downloading files and checking for viruses and potentially unwanted programs bundled with the download.
- Entering contact information into signup forms and checking for resulting spam or a high volume of non-spam emails sent by the site or its affiliates.
- Checking for excessive popup windows.
- Checking for attempts by the site to exploit browser vulnerabilities.
- Checking for deceptive or fraudulent practices employed by a site.

The team assimilates test results into a safety report that can also include:

- Feedback submitted by site owners, which might include descriptions of safety precautions used by the site or responses to user feedback about the site.
- Feedback submitted by site users, which might include reports of phishing scams, bad shopping experiences, and selling services that can be obtained without cost from other sources.
- Additional analysis by McAfee professionals.

Safety icons and balloons protect during searches

When users type keywords into a popular search engine such as Google, Yahoo!, MSN, Ask, or AOL.com, color-coded safety icons appear next to sites listed in the search results page:

 (Green, checkmark)	Tests revealed no significant problems.
 (Yellow, exclamation point)	Tests revealed some issues users should know about. For example, the site tried to change the testers' browser defaults, displayed popups, or sent them a significant amount of non-spam email.
 (Red, x)	Tests revealed some serious issues that users should consider carefully before accessing this site. For example, the site sent testers spam email or bundled adware with a download.
 (Red, bar)	This site is blocked by a policy option.
 (Gray, question mark)	This site is unrated.

Placing the cursor over an icon displays a safety balloon that summarizes the safety report for a site. Click **Read site report** for a detailed safety report.

Using site safety balloons

Use this task to view additional information available through a site's safety icon listed in a search results page.

Task

1. Hold the cursor over the site's safety icon. A safety balloon displays a high-level summary of the site's safety report.
2. For additional details, either:
   - Click **Read site report** in the safety balloon to view details of the site's safety report.
   - Click **Troubleshoot** to test the connection to the SiteAdvisor server when a communication error occurs. No rating for a site might be caused by a broken Internet connection or a problem with the SiteAdvisor server where ratings information is stored.

Testing communication problems

Use this task from a client computer to determine why browser protection is not communicating with the SiteAdvisor server that provides safety ratings information. Communication problems are indicated by a gray SiteAdvisor menu button with disconnected cables.

Before you begin

Be sure that the option for showing safety balloons is enabled. This option is available on the SiteAdvisor menu.

Task

1 Hold your cursor over the SiteAdvisor menu button to display the safety balloon.

2 In the safety balloon, click **Troubleshooting**. Three connectivity tests run to verify that:

- Your computer can connect to the Internet.
- The SiteAdvisor server is running.
- The SiteAdvisor server is responding to safety rating requests.

3 Check the results when they are displayed and follow any instructions to resolve the problem.

4 If you have taken steps to resolve the problem and want to test the connection, click **Repeat Tests**.

SiteAdvisor menu protects while browsing

When users browse to a website, a color-coded menu button appears in the top-left corner of the window. The color of the menu button corresponds to the site's safety rating. Placing the cursor over this button displays a safety balloon that summarizes the safety report for the site, with a link to the detailed site report page. The menu button next to the icon displays the SiteAdvisor menu.

This button...	With this color and symbol...	Indicates this...
	Green, checkmark	The site is safe.
	Yellow, exclamation point	There might be some issues with the site.
	Red, x	There might be some serious issues with the site.
	Gray, question mark	No rating is available for the site.
	Gray, disconnected cables	Your browser is not communicating with the SiteAdvisor website that contains rating information.

Client settings that affect the SiteAdvisor menu button

- When browser protection is disabled, the menu button is gray.
- When visiting a site on your network's intranet, the menu button is gray. Browser protection does not report visits to intranet sites to the SiteAdvisor server.
- When a communication error occurs with the SiteAdvisor server, the menu button is gray with disconnected cables.
- In Internet Explorer, users can display or hide the menu button by using the **View | Toolbars | McAfee SiteAdvisor** menu option. This does not affect the functional status (enabled or disabled) of the browser protection client software.

  NOTE: Firefox users cannot hide the menu button while browser protection is enabled.

Using the SiteAdvisor menu

- Use this task to display menu options for accessing browser protection features.

Task

- Click the down arrow on the SiteAdvisor menu button to view the SiteAdvisor menu.

Select this command...	To do this...
View Site Report	Display the safety report for the current site (not available when browser protection is disabled). NOTE: You can also click **Read site report** in the site safety balloon.
Show Balloon	Display the current site's safety balloon (not available when browser protection is disabled). The balloon disappears after a few seconds, or you can click the close button. NOTE: The site safety balloon also appears by placing the cursor over the menu button.
Disable/Enable SiteAdvisor	Turn the browser protection client software off or on (available only when a policy option is configured to allow this functionality).
About	Access a brief description of browser protection, its license agreement, and its privacy policy.

Safety reports provide details

Users can supplement the color-coded safety information for a site by viewing its detailed safety report. These reports describe specific threats discovered by testing and include feedback submitted by site owners and users.

Safety reports for sites are delivered from the McAfee SiteAdvisor server and provide the following information:

Item	Explanation
Summary	The overall rating for the website. We determine this rating by looking at a wide variety of information. First, we evaluate a website's email and download practices using our proprietary data collection and analysis techniques. Next, we examine the website itself to see if it engages in annoying practices such as excessive pop-ups or requests to change your home page. Then we perform an analysis of its online affiliations to see if the site associates with other sites flagged as red. Finally, we combine our own review of suspicious sites with feedback from our volunteer reviewers and alert you to sites that are deemed suspicious.
Established	The year the domain name was registered. More recently registered websites have had less time to prove their safety and trustworthiness.
Country	The country where a domain is registered. Keep in mind that it's sometimes more difficult to get good customer service or resolve disputes with websites registered outside of your country of residence.
Popularity	The level of how popular the website is. Don't assume, however, that popularity always goes hand in hand with safety. For example, some very popular prize sites send lots of spam, and some very popular file-sharing programs bundle adware. Likewise, many personal websites, blogs and small business sites that

Item	Explanation
	do not get a lot of traffic can be safe to browse and use. That's why the analysis behind SiteAdvisor's overall verdict is so useful.
Email Results	Overall rating for a website's email practices. We rate sites based on both how much email we receive after entering an address on the site as well as how spammy the email we receive looks. If either of these measures is higher than what we consider acceptable, we'll give the site a yellow warning. If both measures are high, or one of them looks particularly egregious, we'll give the site a red warning. Each email link opens a detailed email analysis page.
Downloads	Overall rating about the impact a site's downloadable software had on our testing computer. Red flags are given to sites that have virus-infected downloads or that add unrelated software which many people would consider adware or spyware. The rating also takes note of the network servers a program contacts during its operation, as well as any modifications to browser settings or a computer's registry files. Each download link opens a detailed download analysis page.
Online Affiliations	Indication of how aggressively the site tries to get you to go to other sites that we've flagged as red. It is a very common practice on the Internet for suspicious sites to have many close associates with other suspicious sites. The primary purpose of these "feeder" sites is to get you to visit the suspicious site. A site can receive a red warning if, for example, it links too aggressively to other red sites. In effect, a site can become "red by association" due to the nature of its relationship to red flagged domains.
Annoyances	Common web practices that users find annoying, such as excessive popups, requests to change a user's home page or requests to add a site to the browser's favorites list. We also list 3rd party cookies (sometimes known as "tracking cookies") in this section. If a website has a lot of pop-ups and in particular, if it engages in practices such as popping up more windows when you try to close them, we will give that website a red flag.
Exploits	Rare but extremely dangerous security threats caused by a website "exploiting" a browser's security vulnerability. The exploit can cause the user's computer to receive programming code which can cause adware infections, keystroke spying, and other malicious actions which can leave a computer essentially unusable.
Reviewer and Site Owner Comments	Reviewers and site owners can provide additional information and commentary to supplement SiteAdvisor's automated test results.
Results	Summary of the comments of SiteAdvisor's entire reviewer community. Reviewers can rate sites for downloads, email practices, shopping experiences and more. This input is particularly important in helping the SiteAdvisor community guide each other concerning e-commerce websites. Anonymous input alone is not enough to change a site's overall rating, but sufficient votes from registered users can affect a site's rating.
Website owner comments	Allows owners of analyzed websites to address our ratings. Owners are free to comment, disagree or clarify. These comments are posted unedited after we verify the authenticity of the person leaving the comment. We manually review all owner comments and if an error was made, we will try our best to promptly correct it. We don't allow sites to pay to be rated or to change or improve their ratings.
Reviewer comments	What our volunteer reviewers have to say about this website. These comments are posted unedited.

Viewing safety reports

Use this task to view safety reports to obtain more information about a site's safety rating.

Task

- Do any of the following to view a safety report for a site:

From this location...	Do this...
Website	• Click the SiteAdvisor menu button, then select **View Site Report**. • Hold the cursor over the SiteAdvisor button, then select **Read site report**. • Click the SiteAdvisor button.
Search results page	Click the safety icon following the web page link.
SiteAdvisor home page (www.siteadvisor.com) or Analysis page	Type a URL in the **Look up site report** box.

Information that browser protection sends to McAfee

The client software sends the following information to the SecurityCenter for use in the Web Filtering report:

- Type of event initiated by the client computer (site visit or download).
- Unique ID assigned by Total Protection Service to the client computer.
- Time of event.
- Domain for event.
- URL for event.
- SiteAdvisor rating for the event's site.
- Whether the event's site or site resource is added to the Exceptions list as an authorized or prohibited site.
- Reason for action (allow, warn, or block) taken by browser protection.

Browser protection sends the following information to the SiteAdvisor website's servers:

- Version of the browser protection client software running on the client computer.
- Version of the operating system running on the client computer.
- Language and country locale selected for the operating system and browser running on the client computer.
- Host name and part of the URL for each website the client computer requests to access.
- MD5 algorithm for each application the client computer requests to download.

When a client computer visits a website, browser protection tracks the site's domain specifier. The domain specifier is the smallest amount of information required for browser protection to uniquely identify the site being rated for security. The focus of browser protection is protecting your client computers; no attempt is made to track personal Internet usage.

NOTE: Browser protection does not send information on your company's intranet site to the SiteAdvisor servers.

Installing browser protection during policy updates

Use this task to install browser protection automatically whenever client computers check for an updated policy. You might want to use this feature for adding browser protection on computers where the Total Protection Service client software is already installed. By default, this option is enabled.

Task

For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Browser Protection**, then click the **General Settings** tab.
3. Under Firewall Configuration, select **Automatically install browser protection on all computers using this policy**.
4. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click Save.)

Web filtering features

If you purchased a version of McAfee SaaS Endpoint Protection that includes the web filtering module, the Policies page in the SecurityCenter displays an expanded set of policy options labeled **Browser Protection & Web Filtering**.

The additional policy options enable you to configure these features.

- Regulate user access to websites, based on their safety rating (for example, block access to red sites and display a warning before opening yellow sites).
- Regulate user access to phishing pages.
- Regulate access to site resources, such as file downloads, based on their safety rating.
- Regulate user access to websites based on their content (for example, block access to shopping or gambling sites).
- Create a list of authorized and prohibited sites, based on their URL or domain.
- Customize the message that the browser protection service displays on computers that attempt to access a blocked website.
- Enable and disable the browser protection service at the policy level.
- Specify whether the browser protection service can be disabled from a client computer.

Enabling and disabling browser protection via policy

Use this task to enable and disable the browser protection service on all client computers using the policy.

This feature is available only in versions of the browser protection service that include the web filtering module.

Task

For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Browser Protection & Web Filtering**, then click the **General Settings** tab.
3. Under Browser Protection Status, select or deselect the option **Disable browser protection on all computers using this policy**.

   This feature takes effect on client computers the next time they update their policy.
4. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Enabling and disabling browser protection at the client computer

Use this task to specify whether the browser protection service can be disabled from a client computer.

When this capability is enabled, the **Enable SiteAdvisor** or **Disable SiteAdvisor** option appears on the SiteAdvisor menu.

NOTE: If the browser protection service remains disabled, it is re-enabled automatically the next time the client computer checks for policy updates. (This presumes that the browser protection service is enabled at the policy level.)

This feature is available only in versions of the browser protection service that include the web filtering module.

Task

For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Browser Protection & Web Filtering**, then click the **General Settings** tab.
3. Under Browser Protection Status, select or deselect the option **Allow users to enable or disable browser protection**.
4. Specify whether a password is required on the client computer. If so, type the password.
5. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

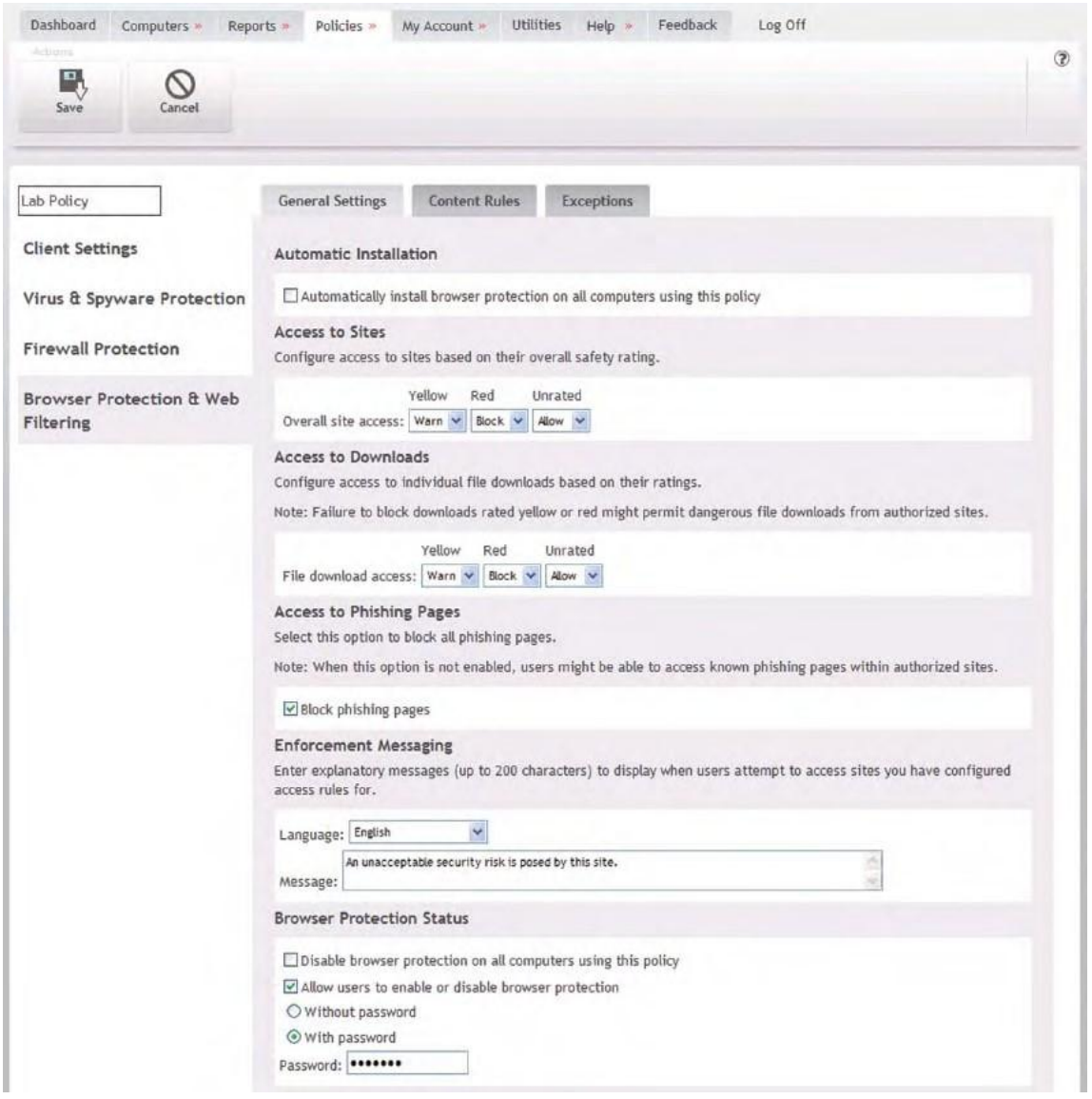
Block and warn sites by safety ratings

Web filtering adds policy options that allow you to use the site safety ratings provided by the browser protection service to determine whether users can access a site or resources on a site, such as download files.

- For each yellow, red, or unrated site, specify whether to allow, warn, or block the site.
- For each yellow, red, or unrated download file, specify whether to allow, warn, or block the download. This enables a greater level of granularity in protecting

users against individual files that might pose a threat on sites with an overall green rating.

- For each phishing page, specify whether to block or allow access. This enables a greater level of granularity in protecting users from pages that employ phishing techniques on a site with an overall green rating.



When you block a site, users are redirected to a message explaining that the site is blocked. A policy option allows you to customize the message that is displayed.

When you configure a warning action for a site, users are redirected to a message explaining that there might be threats on the site. They can then decide whether to cancel or continue their navigation to the site.

NOTE: To ensure users can access specific sites that are important to your business, no matter how they are rated, add them to the Exceptions list as an authorized site. For authorized sites, the browser protection service ignores the safety rating.

Blocking or warning site access based on safety ratings

Use this task to block users from accessing sites that contain threats or to warn users about potential threats on sites.

This feature is available only in versions of the browser protection service that include the web filtering module.

Task

For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Browser Protection & Web Filtering**, then click the **General Settings** tab.
3. Under Access to Sites, select a separate level of access for red, yellow, and unrated sites.
   - **Block** — Block access to all sites with the specified rating.
   - **Warn** — Display a warning when users attempt to access a site with the specified rating.
   - **Allow** — Allow access to all sites with the specified rating.
4. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Blocking or warning file downloads based on safety ratings

Use this task to block users from downloading files that contain threats or to warn users about potential threats from downloads.

A site with an overall safety rating of green can contain individual download files rated yellow or red. To protect users, specify an action that is specific to the rating for an individual file.

This feature is available only with versions of the browser protection service that include the web filtering module.

NOTE: This feature is not available in Firefox browsers because Firefox is unable to recognize safety ratings for individual site resources.

Task

For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Browser Protection & Web Filtering**, then click the **General Settings** tab.
3. Under Access to Downloads, select a separate level of access for red, yellow, and unrated sites.
   - **Block** — Block all downloads of files with the specified rating.
   - **Warn** — Display a warning when users attempt to download a file with the specified rating.
   - **Allow** — Allow downloads of files with the specified rating.
4. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Blocking phishing pages

A site with an overall safety rating of green can contain phishing pages. To protect users, use this web filtering task to block access to these pages.

This feature is available only with versions of the browser protection service that include the web filtering module.

Task

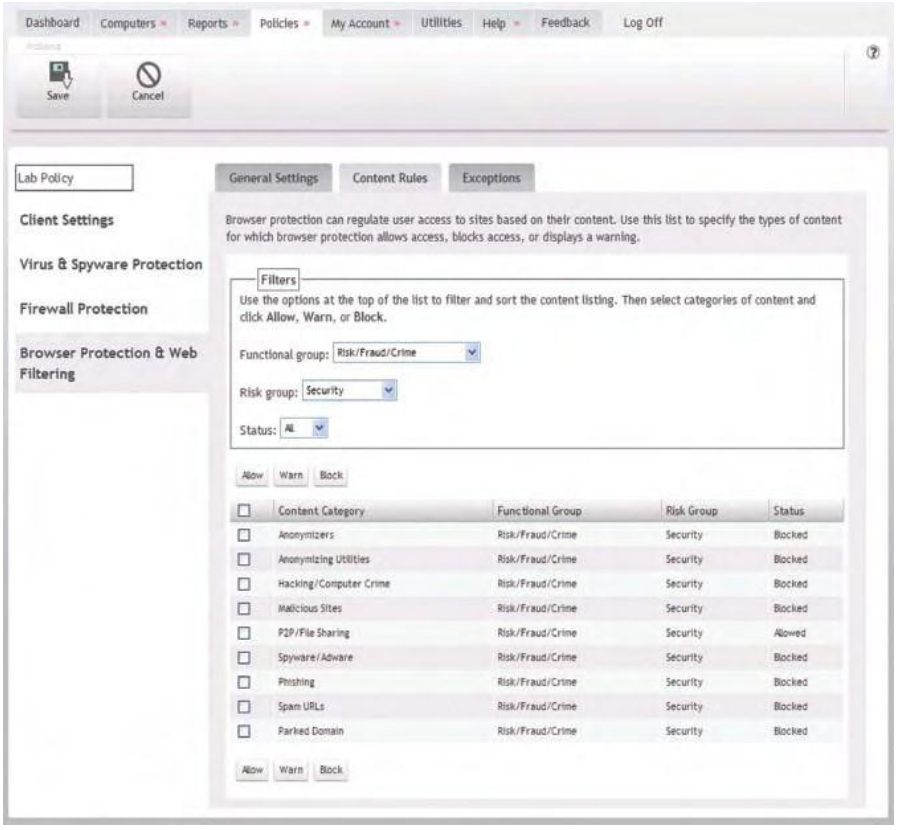
For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Browser Protection & Web Filtering**, then click the **General Settings** tab.
3. Under Access to Phishing Pages, select **Block phishing pages**.
4. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Block and warn sites by content

Web filtering allows the browser protection service to retrieve content classifications for a site. These are stored on the server maintained by McAfee where site safety ratings information is also stored. Use policy options to allow, warn, or block access to sites based on the type of content they contain.

This feature is available only with versions of the browser protection service that include the web filtering module.



The approximately 100 site content categories are grouped by function and risk, which allows for easy application of the policy settings based on content alone or on content functional groups (the functions that users can perform by accessing the content) or content risk groups (the risks that the content might present to your business).

For example, select a functional group of Risk/Fraud/Crime and a risk group of Security to view all the categories of content that might pose a threat to user security due to fraud or criminal intent. Select a risk group of Productivity to display all the categories of content that might impact users' productivity adversely, such as shopping or gaming. These filters assist you in locating all the content categories for which you might want to configure actions.

Blocking or warning site access based on content

Use this task to block users from accessing sites that contain particular types of content.

This feature is available only with versions of the browser protection service that include the web filtering module.

Task

For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Browser Protection & Web Filtering**, then click the **Content Rules** tab.
3. Select one or more filtering options to customize the content categories listed. *(Optional)*
   - **Functional group** — Display content categories that are used to perform similar functions.
   - **Risk group** — Display content categories that present similar risks to users.
   - **Action** — Display the content categories for which you have configured an allow, block, or warn action.
4. In the list, select the content categories for which you want to select an action.
5. Click **Allow**, **Block**, or **Warn**. This action will be applied when users attempt to access websites that contain the selected categories of content.
6. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Authorize and prohibit sites by URL or domain

Web filtering allows you to set up an Exceptions list containing a list of sites that users can or cannot access.

- Authorized sites that users are always allowed to access, regardless of their safety rating or type of content. Add authorized sites to ensure access to sites that are important to your business.
- Prohibited sites that users are never allowed to access. Add prohibited sites to block access to sites that are not related to job performance or do not conform to company security standards.

NOTE: By authorizing a site, the browser protection service ignores the safety rating for that site. Users can access authorized sites even if threats have been reported on these sites and they have a safety rating of red. Users can also access unsafe downloads and phishing pages on authorized sites. It is important to exercise caution when adding authorized sites to an Exceptions list.

How site patterns work

The Exceptions list uses site patterns to specify a range of sites that are authorized or prohibited. This enables you to authorize or prohibit a particular domain or a range of similar sites without entering each URL separately.

When a client computer attempts to navigate to a site, the browser protection service checks whether the URL matches any site patterns configured in the Exceptions list. It uses specific criteria to determine a match.

A site pattern consists of a URL or partial URL, which the browser protection service interprets as two distinct sections: domain and path.

Site pattern: www.mcafee.com/us/enterprise	
http:// www.mcafee.com	This is the **domain**. The domain consists of two parts: • **Protocol.** In this case: **http://** • **Internet domain.** In this case: **www.mcafee.com** Domain information is matched from the *end*. A matching URL's domain must *end* with the site pattern's domain. The protocol can vary. These domains match: • http:// ftp.mcafee.com • https://mcafee.com • http://www.info.mcafee.com These domains do not match: • http:// www.mcafee.downloads.com • http://mcafee.net • http://www.mcafeeasap.com • http://us.mcafee.com
/us/enterprise	This is the **path**. The path includes everything that follows the / after the domain. Path information is matched from the *beginning*. A matching URL's path must *begin* with the site pattern's path. These paths match: • /us/enterpriseproducts • /us/enterprise/products/security These paths do not match: • /emea/enterprise • /info/us/enterprise

Site patterns must be at last six characters in length, and they do not accept wildcard characters. The browser protection service does not check for matches in the middle or end of URLs.

Use the "." character at the beginning of a site pattern to match a specific domain. For convenience, the "." character disregards the protocol and introductory characters.

Example: **.mcafee.com**

Matches	Does not match
• http://www.info.mcafee.com • http://mcafee.com • http://ftp.mcafee.com	http://www.mcafeeasap.com • http://salesmcafee.com • http://ftp.mcafee.net

•

Adding authorized and prohibited sites

Use this web filtering task to create and manage an Exceptions list for browser protection.

An Exceptions list contains:

- Authorized sites that users are always allowed to access.
- Prohibited sites that users are never allowed to access.

This feature is available only with versions of the browser protection service that include the web filtering module.

Task

For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Browser Protection & Web Filtering**, then click the **Exceptions** tab.
3. Click **Add to Exceptions List**.
4. Type a URL or site pattern into the text box, then click an action to associate with the site.
   - **Authorize** — Add the site to the Exceptions list as an authorized site, which users are always allowed to access.
   - **Prohibit** — Add the site to the Exceptions list as a prohibited site, which users are not allowed to access.
   - **Cancel** — Close the text box without adding the site to the list.
5. Repeat step 4 for each site you want to add to the list**.**
6. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Customizing messages for users

Use this task to create a message that displays when users attempt to access sites that are blocked.

The message appears when users attempt to access a site you have blocked by ratings, by content, or by adding it to the Exceptions list as a prohibited site. Instead of navigating to the site, users are redirected to a page displaying the customized message. You might use the message to explain why the site is blocked.

The message appears on client computers in the language configured for the client software, if you have created the message in that language.

This feature is available only with versions of the browser protection service that include the web filtering module.

Task

For option definitions, click **?** in the interface.

1. On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Select **Browser Protection & Web Filtering**, then click the **General Settings** tab.
3. Under Enforcement Messaging, select a language for the message. (By default, the language in which you have logged in appears. If that language is not available for messages, English is displayed.)
4. Type a message of up to 200 characters.
5. Repeat steps 3 and 4 for each language for which you want to configure a message.
6. Click **Save**. (For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Viewing browsing activity

Use this task to view the Web Filtering report, which lists visits to websites by client computers and attempts to access websites for which you have configured policy options to regulate access.

Task

1. Click the **Reports** tab, then click **Web Filtering.**
2. In the Web Filtering report, view the number of green sites visited by client computers on the network. No detailed information is available for green sites.
3. For yellow and red sites, do any of the following**.**

When you want to...	Do this...
Display the sites in a domain	Click the triangle icon next to the domain name to display the sites users attempted to access in the domain.
View details about an access attempt	Click a quantity to display the Event Details page: • When **View | Computers** is selected, click a quantity in an action column (such as **Blocked**). • When **View | Domains** is selected, click a quantity under **Access Count**. The Event Details page shows the name of the computer that attempted to access the site, the URL for the site, the type of access attempted, and the date and time of the attempted access.
View details about a computer	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.

See also

Information that browser protection sends to McAfee on page 107
Web Filtering report on page 117

Web Filtering report

Use the Web Filtering report, available from the SecurityCenter, to track Internet usage and browsing activity on your network.

This report lists visits to websites and attempts to access websites for which you have configured policy options to regulate access. Use this report to view detailed information about the specific sites, their safety ratings and content categories, the computers that attempted to access them, and the action taken by browser protection.

This report is available only with versions of the browser protection service that include the web filtering module.

See also

Viewing browsing activity on page 116
Information that browser protection sends to McAfee on page 107

Best practices (browser protection)

To develop an effective strategy for guarding against web-based threats, we recommend that you proactively track browsing activity on your network and configure policy options appropriate for your users.

1. Check your status emails or the SecurityCenter website for an overview of your account's status. Ensure that browser protection is installed and enabled on all computers.
2. Check the Web Filtering report regularly to see what sites users are visiting, their safety ratings, and their content categories.
3. Using the Web Filtering report:
   - Determine whether users are visiting sites that should be added to an Exceptions list. Authorize sites that are important to productivity to ensure that users can always access them. Prohibit sites that do not comply with company policy or contribute to job performance goals to ensure users cannot access them.
   - Note the number of visits to red, yellow, and unrated sites. If appropriate, configure policy options to block sites or site resources that have particular safety ratings.
   - Note the content categories for sites being visited. If appropriate, configure policy options to block sites containing particular types of content.
   - Note which computers are visiting which sites. If appropriate, configure different policies for computers that should and should not be able to access particular sites or content.
4. Customize a message to display on client computers that attempt to access a site you have blocked.
5. To ensure that all computers are protected against web-based threats, configure policy options to enable browser protection via policy and prevent users from disabling browser protection on their computers.

Frequently asked questions

This section includes questions asked by administrators and client computer users that are related to using the features of browser protection.

Can I run browser protectionfor Internet Explorer and Firefox on the same computer?

Yes. Browser protection for Internet Explorer and Firefox are compatible on the same computer. You can install protection for both browsers. (If both browsers are present on a computer when browser protection is installed, protection for both browsers is installed automatically.)

If Microsoft Internet Explorer is the only browser installed on a client computer when browser protection is installed, does browser protection need to be reinstalled after installing Mozilla Firefox?

No. The browser protection client software detects Firefox when it is installed and immediately begins to protect searching and browsing activities in that browser, while continuing to provide protection for Internet Explorer.

How does browser protection define a website visit? Does browser protection track individual website pages viewed on managed systems?

When a client computer visits a website, browser protection tracks the site's domain specifier. The domain specifier is the smallest amount of information required for browser protection to uniquely identify the site being rated for security. For example, if a client computer visited 10 different pages on this website over the course of a single browser session:
www.mcafee.com

only a single visit would be logged to this domain:

.mcafee.com

That is the information required to locate a safety rating. A single browser session times out after 30 minutes, and a new session is then tracked.

Why is the SiteAdvisor button gray?

Several causes are possible:

- The site is not rated. Visit the www.siteadvisor.com website to submit a website for testing.
- The browser protection client software is disabled. Click the arrow on the menu button to display the SiteAdvisor menu, then select **Enable SiteAdvisor**. (If browser protection is already enabled, the menu option changes to **Disable SiteAdvisor**. These menu options appear only if the policy assigned to the computer enables them.)
- The site is on your local intranet. Browser protection does not report information about intranet sites to the SiteAdvisor server for ratings purposes.
- Proxy server settings are configured incorrectly. Authentication support in Total Protection Service is limited to anonymous authentication or Windows domain challenge/response authentication. Basic authentication is not supported.
- The client computer is not communicating with the SiteAdvisor server. A communication error icon (disconnected cables) appears on the SiteAdvisor button. Hold your cursor over the menu button to display the safety balloon, then click **Troubleshooting** to test the connection.